

FIG.1

STRICTLY CONFIDENTIAL DOCUMENT:

Prohibited from copying in principle (authorization of administrator required upon copying), and the copying required to be recorded;

Watermark indicating copy-prohibition required to be applied upon printing, and the printing required to be recorded;

Only person involved allowed for browsing.

CLASSIFIED DOCUMENT:

Only person involved allowed to copy;

Label indicating Classified Document required to be printed as well upon printing;

Only person involved allowed for browsing.

INTERNAL-USE-ONLY DOCUMENT:

Authorization of administrator required upon sending externally;

No authorization required for copying, printing and browsing internally.

HUMAN-RESOURCE RELATED DOCUMENT:

All treated as Classified Document.

FIG.2

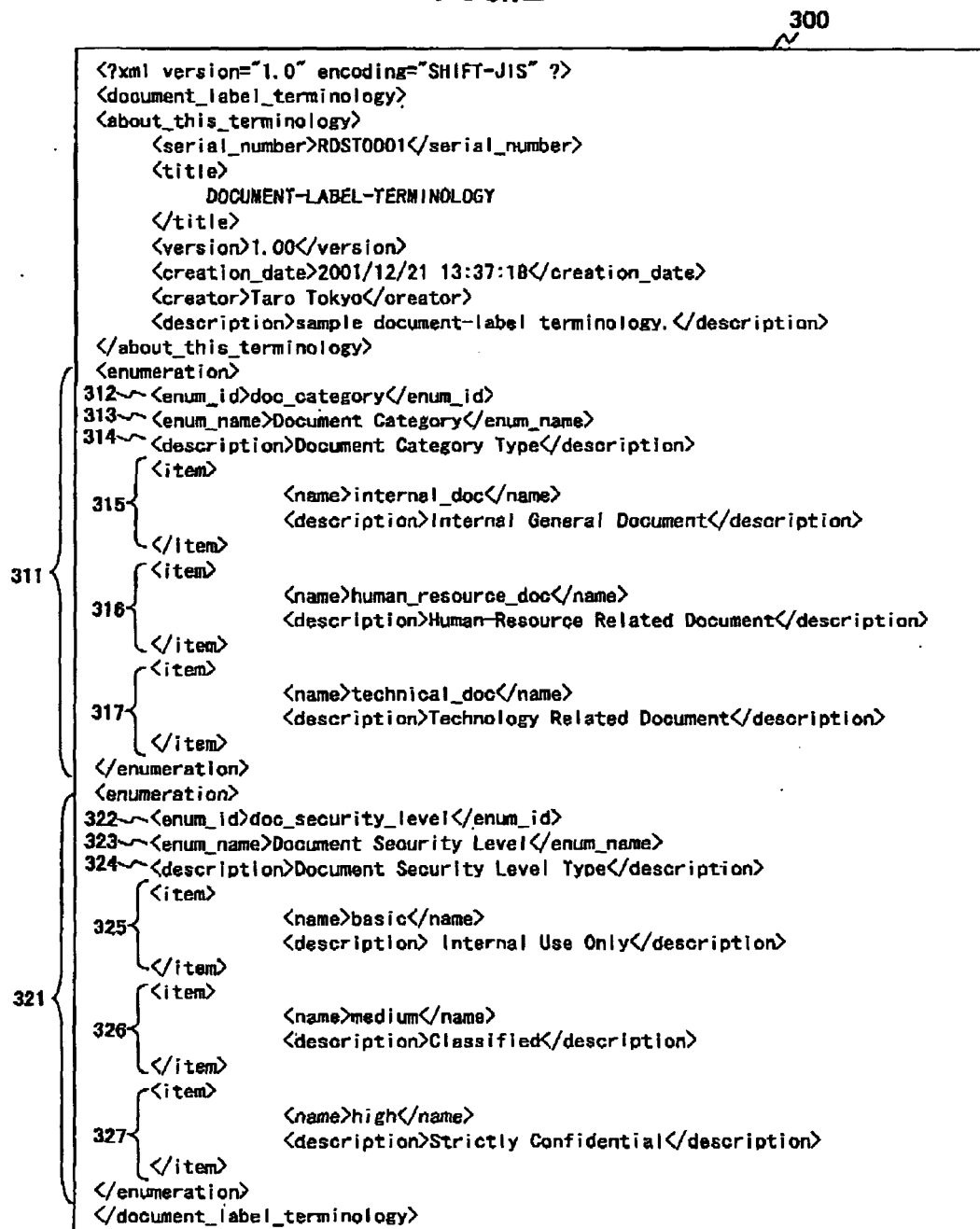


FIG.3

400

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
  <about_this_terminology>
    <serial_number>RDST9487</serial_number>
    <title>DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
    <version>1.00</version>
    <creation_date>2001/12/21 13:37:18</creation_date>
    <creator>Taro Tokyo</creator>
    <description>sample policy terminology.</description>
  </about_this_terminology>

  <!-- Enumeration of System Types-->
  <enumeration>
    <enum_id>system_type</enum_id>
    <enum_name>System Type</enum_name>
    <description>System Type</description>
    <item>
      <name>Copier</name>
      <description>Copier</description>
      <operation>copier_operation</operation>
    </item>
    <item>
      <name>Printer</name>
      <description>Printer</description>
      <operation>printer_operation</operation>
    </item>
    <item>
      <name>Facsimile</name>
      <description>Facsimile</description>
      <operation>fax_operation</operation>
    </item>
    <item>
      <name>Scanner</name>
      <description>Scanner</description>
      <operation>scanner_operation</operation>
    </item>
    <item>
      <name>Document Repository</name>
      <description>Document Repository</description>
      <operation>repository_operation</operation>
    </item>
    <item>
      <name>E-Meeting</name>
      <description>Electronic Meeting System</description>
      <operation>meeting_operation</operation>
    </item>
  </enumeration>
```

411

FIG.4

```
400 { ~
    <!-- Enumeration of Operations for Each System Type-->
    <enumeration>
      <enum_id>copier_operation</enum_id>
      <enum_name>Copier Operation</enum_name>
      <description>Operation Regarding Copier</description>
      <item>
        <name>hardcopy</name>
        <description>Copy from Paper to Paper</description>
        <requirement>hardcopy_requirement</requirement>
      </item>
    </enumeration>
    <enumeration>
      <enum_id>printer_operation</enum_id>
      <enum_name>Printer Operation</enum_name>
      <description>Operation Regarding Printer</description>
      <item>
        <name>print</name>
        <description>Print Electronic Document on Paper</description>
        <requirement>print_requirement</requirement>
      </item>
    </enumeration>
    <enumeration>
      <enum_id>fax_operation</enum_id>
      <enum_name>Facsimile Operation</enum_name>
      <description>Operation Regarding Fax</description>
      <item>
        <name>fax_send</name>
        <description>Send Fax</description>
        <requirement>fax_send_requirement</requirement>
      </item>
      <item>
        <name>fax_receive</name>
        <description>Receive Fax</description>
        <requirement>fax_receive_requirement</requirement>
      </item>
    </enumeration>
    <enumeration>
      <enum_id>scanner_operation</enum_id>
      <enum_name>Scanner Operation</enum_name>
      <description>Operation Regarding Scanner</description>
      <item>
        <name>scan</name>
        <description>Scan Paper Document into Electronic Document</description>
        <requirement>scan_requirement</requirement>
      </item>
    </enumeration>
  ~
```

421 {

431 {

441 {

451 {

FIG.5

```
400 ~
<enumeration>
  <enum_id>repository_operation</enum_id>
  <enum_name>Document Repository Operation</enum_name>
  <description>Operation Regarding Document Repository</description>
  <item>
    <name>store</name>
    <description>Store</description>
    <requirement>store_requirement</requirement>
  </item>
  <item>
    <name>revise</name>
    <description>Revise/Edit</description>
    <requirement>revise_requirement</requirement>
  </item>
  <item>
    <name>delete</name>
    <description>Delete/Abandon</description>
    <requirement>delete_requirement</requirement>
  </item>
  <item>
    <name>read</name>
    <description>Read</description>
    <requirement>read_requirement</requirement>
  </item>
  <item>
    <name>net_delivery</name>
    <description>
      Deliver (Transmit) via Network
    </description>
    <requirement>net_delivery_requirement</requirement>
  </item>
  <item>
    <name>disc_delivery</name>
    <description>Deliver (Send) via Disk</description>
    <requirement>disc_delivery_requirement</requirement>
  </item>
  <item>
    <name>archive</name>
    <description>Archive/Backup</description>
    <requirement>archive_requirement</requirement>
  </item>
</enumeration>
461 ~
<enumeration>
  <enum_id>emeeting_operation</enum_id>
  <enum_name>E-Meeting Operation</enum_name>
  <description>Operation Regarding Electronic Meeting System</description>
  <item>
    <name>meeting_use</name>
    <description>Use at Meeting</description>
    <requirement>meeting_use_requirement</requirement>
  </item>
</enumeration>
471 ~
```

FIG.6

```
400 ~~~~~
<!-- Enumeration of Requirements Applicable for Each Operation-->
<!-- User Authentication, Document Identification, Access Control (Use Limitation) are
provided as Basic Mechanism and not included in Requirements-->
<enumeration>
  <enum_id>hardcopy_requirement</enum_id>
  <enum_name>Hardcopy Requirement</enum_name>
  <description>Requirements on Copying</description>
  <item>
    <name>explicit_authorization</name>
    <description>Explicit Authorization</description>
  </item>
481 <item>
    <name>audit</name>
    <description>Record Audit Trail</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>Record Audit Trail with Image</description>
  </item>
</enumeration>
<enumeration>
  <enum_id>print_requirement</enum_id>
  <enum_name>Print Requirement</enum_name>
  <description>Requirements on Printing</description>
  <item>
    <name>explicit_authorization</name>
    <description>Explicit Authorization (Use Limitation)</description>
  </item>
  <item>
    <name>audit</name>
    <description>Record Audit Trail</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>Record Audit Trail with Image</description>
  </item>
481 <item>
    <name>private_access</name>
    <description>Paper-Output by One Who Prints</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>
      Use Trusted Channel (Encrypt Print Data)
    </description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      Embed Trace Information in Printout (Watermark, Label, Bar Code)
    </description>
  </item>
</enumeration>
~~~~~
```

FIG. 7

400

```
<enumeration>
  <enum_id>fax_send_requirement</enum_id>
  <enum_name>Requirement on Sending Fax Message</enum_name>
  <description>Requirements on Sending Fax Message</description>
  <item>
    <name>exploit_authorization</name>
    <description>Explicit Authorization (Use Limitation)</description>
  </item>
  <item>
    <name>audit</name>
    <description>Record Audit Trail</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>Record Audit Trail with Image</description>
  </item>
  <item>
    <name>destination_restriction</name>
    <description>Destination Restriction</description>
  </item>
  <item>
    <name>private_mode</name>
    <description>Transmit in Private Mode</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>
      Use Trusted Channel
    </description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      Embed Trace Information in Sent Fax (Watermark, Label, Bar Code)
    </description>
  </item>
  <item>
    <name>non_repudiation</name>
    <description>Prevent Repudiation (Acquire Return Receipt)</description>
  </item>
</enumeration>
```

501

FIG.8

```
400 {
    <enumeration>
      <enum_id>fax_receive_requirement</enum_id>
      <enum_name>Requirement on Receiving Fax Message</enum_name>
      <description>Requirements on Receiving Fax Message</description>
      <item>
        <name>audit</name>
        <description>Record Audit Trail</description>
      </item>
      <item>
        <name>audit_with_image</name>
        <description>Record Audit Trail with Image</description>
      </item>
      <item>
        <name>private_access</name>
        <description>Take out Private Fax by One Addressed To</description>
      </item>
      <item>
        <name>trusted_timestamp</name>
        <description>Trusted Timestamp</description>
      </item>
      <item>
        <name>embed_trace_info</name>
        <description>
          Embed Trace Information in Received Fax (Watermark, Label, Bar Code)
        </description>
      </item>
    </enumeration>
    <enumeration>
      <enum_id>scan_requirement</enum_id>
      <enum_name>Scan Requirement</enum_name>
      <description>Requirements on Scanning (Requirements on Storing are applied after storing)
      </description>
      <item>
        <name>explicit_authorization</name>
        <description>Explicit Authorization (Use Limitation)</description>
      </item>
      <item>
        <name>audit</name>
        <description>Record Audit Trail</description>
      </item>
      <item>
        <name>audit_with_image</name>
        <description>Record Audit Trail with Image</description>
      </item>
      <item>
        <name>embed_trace_info</name>
        <description>
          Embed Trace Information in Scanned Image (Watermark, Label, Bar Code)
        </description>
      </item>
    </enumeration>
  }
511 {
  }
521 {
  }
```

FIG.9

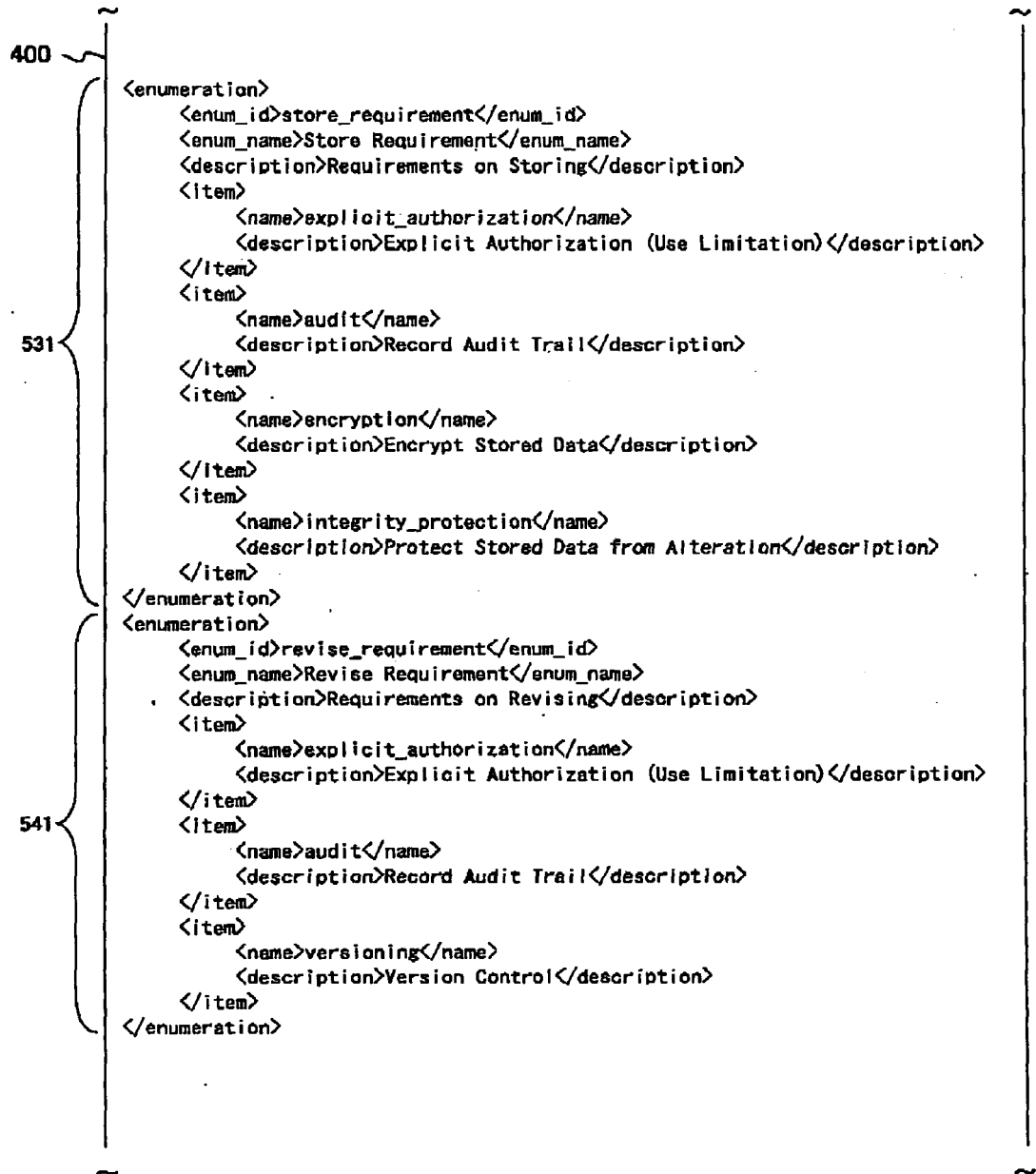


FIG. 10

```
400 { <enumeration>
    <enum_id>delete_requirement</enum_id>
    <enum_name>Delete Requirement</enum_name>
    <description>Requirements on Deleting/Abandoning</description>
    <item>
        <name>explicit_authorization</name>
        <description>Explicit Authorization (Use Limitation)</description>
    </item>
    <item>
        <name>audit</name>
        <description>Record Audit Trail</description>
    </item>
    <item>
        <name>audit_with_image</name>
        <description>Record Audit Trail with Image</description>
    </item>
    <item>
        <name>complete_erase</name>
        <description>Complete Erase</description>
    </item>
</enumeration>
551 { <enumeration>
    <enum_id>read_requirement</enum_id>
    <enum_name>Read Requirement</enum_name>
    <description>Requirements on Reading</description>
    <item>
        <name>explicit_authorization</name>
        <description>Explicit Authorization (Use Limitation)</description>
    </item>
    <item>
        <name>audit</name>
        <description>Record Audit Trail</description>
    </item>
    <item>
        <name>edit_restriction</name>
        <description>Authorization for Reading Only Edition-Prohibited Data</description>
    </item>
    <item>
        <name>print_restriction</name>
        <description>Authorization for Reading Only Print-Prohibited Data</description>
    </item>
    <item>
        <name>location_restriction</name>
        <description>Authorization for Reading Only Reading-Location-Restricted Data</description>
    </item>
    <item>
        <name>user_restriction</name>
        <description>Authorization for Reading Only User-Restricted Data</description>
    </item>
</enumeration>
581 {
```

FIG.11

400

```
<enumeration>
  <enum_id>net_delivery_requirement</enum_id>
  <enum_name>Delivery via Network Requirement</enum_name>
  <description>Requirements on Delivering (Transmitting) via Network</description>
  <item>
    <name>explicit_authorization</name>
    <description>Explicit Authorization (Use Limitation)</description>
  </item>
  <item>
    <name>audit</name>
    <description>Record Audit Trail</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>Record Audit Trail with Image</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>Use Trusted Channel (Encrypt Transmitted Data)</description>
  </item>
  <item>
    <name>destination_restriction</name>
    <description>Destination Restriction (such as Internal Delivery Only)</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>Authorization for Delivering Only Edition-Prohibited Data</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>Authorization for Delivering Only Print-Prohibited Data</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>Authorization for Delivering Only Reading-Location-Restricted Data</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>Authorization for Delivering Only User-Restricted Data</description>
  </item>
</enumeration>
```

571

FIG.12

400

581

```
<enumeration>
  <enum_id>disc_delivery_requirement</enum_id>
  <enum_name>Delivery via Disc Requirement</enum_name>
  <description>Requirements on Delivering (Sending) via Disk</description>
  <item>
    <name>explicit_authorization</name>
    <description>Explicit Authorization (Use Limitation)</description>
  </item>
  <item>
    <name>audit</name>
    <description>Record Audit Trail</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>Record Audit Trail with Image</description>
  </item>
  <item>
    <name>encryption</name>
    <description>Encrypt Sent Data</description>
  </item>
  <item>
    <name>integrity_protection</name>
    <description>Protect Sent Data from Alteration</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>Authorization for Sending Only Edition-Prohibited Data</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>Authorization for Sending Only Print-Prohibited Data</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>Authorization for Sending Only Reading-Location-Restricted Data</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>Authorization for Sending Only User-Restricted Data</description>
  </item>
</enumeration>
```

FIG.13

```
400 {
    <enumeration>
      <enum_id>archive_requirement</enum_id>
      <enum_name>Archive Requirement</enum_name>
      <description>Requirements on Archiving/Backing-up</description>
      <item>
        <name>explicit_authorization</name>
        <description>Explicit Authorization (Use Limitation)</description>
      </item>
      <item>
        <name>audit</name>
        <description>Record Audit Trail</description>
      </item>
      <item>
        <name>encryption</name>
        <description>Encrypt Archived Data</description>
      </item>
      <item>
        <name>integrity_protection</name>
        <description>Protect Archived Data from Alteration</description>
      </item>
    </enumeration>
    <enumeration>
      <enum_id>meeting_use_requirement</enum_id>
      <enum_name>Meeting-use Requirement</enum_name>
      <description>Requirements on Using at Meeting</description>
      <item>
        <name>explicit_authorization</name>
        <description>Explicit Authorization (Use Limitation)</description>
      </item>
      <item>
        <name>audit</name>
        <description>Record Audit Trail</description>
      </item>
      <item>
        <name>audit_with_image</name>
        <description>Record Audit Trail with Image</description>
      </item>
    </enumeration>
  </policy_terminology>
}
```

591 {

601 {

FIG.14

```
2000 ~
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
  <about_this_policy>
    <serial_number>RDSP2023</serial_number>
    <terminology_applied>RDST9487</terminology_applied>
    <title>DOCUMENT-SECURITY-POLICY</title>
    <version>1.30</version>
    <creation_date>2002/02/18 22:30:24</creation_date>
    <creator>Taro Tokyo</creator>
    <description>sample document security policy.</description>
  </about_this_policy>
2001 ~ </policy>
  <acc_rule>~2011
2013 { <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
2017 { <user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <allowed/><!-- allowed without any requirement -->
      </operation>
      <operation>
        <name>print</name>
        <allowed/><!-- allowed without any requirement -->
      </operation>
      <operation>
        <name>fax_send</name>
        <requirement>audit</requirement>
        <requirement>explicit_authorization</requirement>
      </operation>
      <operation>
        <name>fax_receive</name>
        <allowed/><!-- allowed without any requirement -->
      </operation>
      <operation>
        <name>scan</name>
        <allowed/><!-- allowed without any requirement -->
      </operation>
    }
  }
~
```

FIG.15

2000 ~

```
<operation>
  <name>store</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>revise</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>delete</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>read</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>net_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
  <requirement>trusted_channel</requirement>
</operation>
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>meeting_use</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
</ace>
</aol>
</acc_rule> ~ 2012
```

FIG.16

2000

```
<acc_rule>~2021
2023 { <doc_category>ANY</doc_category>
      <doc_security_level>medium</doc_security_level>
      <acl>
        <ace>
          2027 { <user_category>DOC-CATEGORY</user_category>
                 <user_security_level>ANY</user_security_level>
                 <operation>
                   <name>hardcopy</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
                 </operation>
                 <operation>
                   <name>print</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
                 </operation>
                 <operation>
                   <name>fax_send</name>
                   <denied/>
                   <!-- denied even if it is explicitly authorized -->
                 </operation>
                 <operation>
                   <name>fax_receive</name>
                   <allowed/><!-- allowed without any requirement -->
                 </operation>
                 <operation>
                   <name>scan</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
                 </operation>
                 <operation>
                   <name>store</name>
                   <allowed/><!-- allowed without any requirement -->
                 </operation>
               }
        }
      }
    }
```

FIG.17

2000

```
<operation>
  <name>revise</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>delete</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>read</name>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
  <requirement>trusted_channel</requirement>
</operation>
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>meeting_use</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
</ace>
```

FIG.18

2000

```
<ace>
2028 { <user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_send</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_receive</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>scan</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>store</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>revise</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>delete</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
    }
```

FIG.19

2000

```

<operation>
  <name>read</name>
  <requirement>explicit_authorization</requirement>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>disc_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>archive</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>meeting_use</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
</ace>
</acl>
</acc_rule> ~ 2022
<acc_rule> ~ 2031
2033 { <doc_category>ANY</doc_category>
      <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        2037 { <user_category>DOC-CATEGORY</user_category>
              <user_security_level>ANY</user_security_level>
              <operation>
                <name>hardcopy</name>
                <denied/>
                <!-- denied even if it is explicitly authorized -->
              </operation>
              <operation>
                <name>print</name>
                <requirement>explicit_authorization</requirement>
                <requirement>audit</requirement>
                <requirement>private_access</requirement>
                <requirement>trusted_channel</requirement>
                <requirement>embed_trace_inf </requirement>
              </operation>
            }
          }
        }
      }
    }
  }

```

FIG.20

2000

```
<operation>
  <name>fax_send</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>fax_receive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>scan</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>store</name>
  <requirement>audit</requirement>
  <requirement>encryption</requirement>
  <requirement>integrity_protection</requirement>
</operation>
<operation>
  <name>revise</name>
  <requirement>versioning</requirement>
</operation>
<operation>
  <name>delete</name>
  <requirement>complete_erase</requirement>
</operation>
<operation>
  <name>read</name>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
  <requirement>user_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
```

FIG.21

2000

```
<operation>
  <name>diso_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>encryption</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <requirement>encryption</requirement>
  <requirement>integrity_protection</requirement>
</operation>
<operation>
  <name>meeting_use</name>
  <requirement>explicit_authorization</requirement>
</operation>
</ace>
<ace>
2038 { <user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_send</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_receive</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>scan</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
    }
  </ace>
```

FIG.22

2000

```
<operation>
  <name>store</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>revise</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>delete</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>read</name>
  <requirement>explicit_authorization</requirement>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
  <requirement>user_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>disc_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>archive</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>meeting_use</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
```

</ace>

</acl>

</acc_rule> 2032

2002 </policy>

</document_security_policy>

FIG.23

210
~

```
<about_this_policy>
  211 ~<serial_number>RDSP2023</serial_number>
  212 ~<terminology_applied>RDST9487</terminology_applied>
      { <title>DOCUMENT-SECURITY-POLICY</title>
        <version>1.20</version>
        213 { <creation_date>2002/02/18 22:30:24</creation_date>
              <creator>Taro Tokyo</creator>
              <description>ample document security policy</description>
            }
      }
</about_this_policy>
```

FIG.24

220
~

```
<policy>
221 ~<acc_rule>
    232 { <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
    223 ~<acl>
        224 ~<ace>
            225 ~<user_category>DOC-CATEGORY
                </user_category>
            226 ~<user_security_level>ANY
                </user_security_level>
            227 ~<operation>
                228 ~<name>fax_send</name>
                229 ~<denied/><!-- denied even if it
                    is explicitly authorized -->
                </operation>
            227 ~<operation>
                <name>net_delivery</name>
                230 ~<requirement>audit
                    </requirement>
                231 ~<requirement>
                    explicit_authorization
                </requirement>
                ...
            </operation>
            227 ~<operation>
                <name>fax_receive</name>
                232 ~<allowed/><!--allowed
                    without requirements -->
            </operation>
            ...
        </ace>
        224 ~<ace>
            ...
        </ace>
    </acl>
</acc_rule>
221 ~<acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
        ...
    </acl>
</acc_rule>
</policy>
```

FIG.25

240

```
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        241~<denied_operations>
          <!-- denied even if it is explicitly
            authorized -->
          <name>fax_send</name>
        </denied_operations>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          242~<requirement>explicit_authorization
            </requirement>
          ...
        </operation>
        <operation>
          ...
        </operation>
        243~<allowed_operations> <!-- allowed without
          requirements -->
          <name>fax_receive</name>
          <name>store</name>
          ...
        </allowed_operations>
      </ace>
      <ace>
        ...
      </ace>
      ...
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      ...
    </acl>
  </acc_rule>
</policy>
```

FIG.26

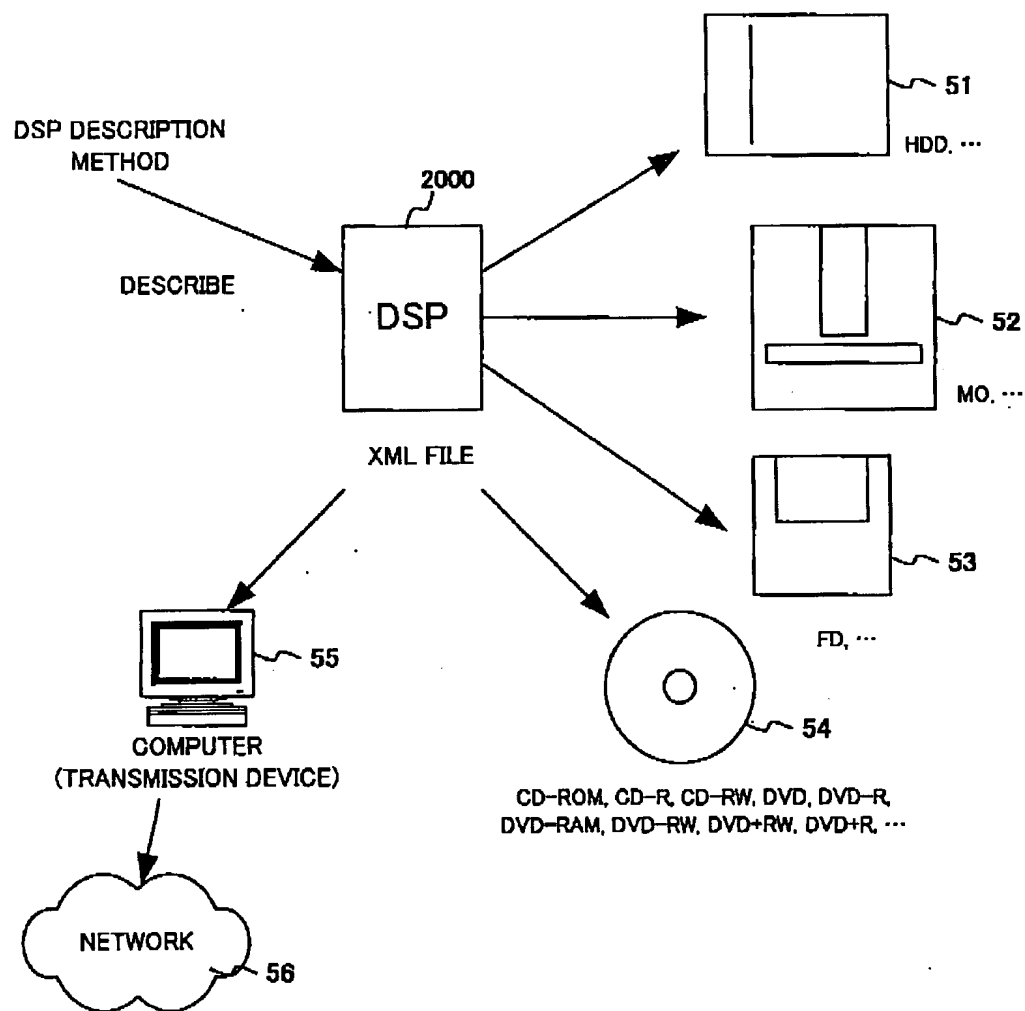
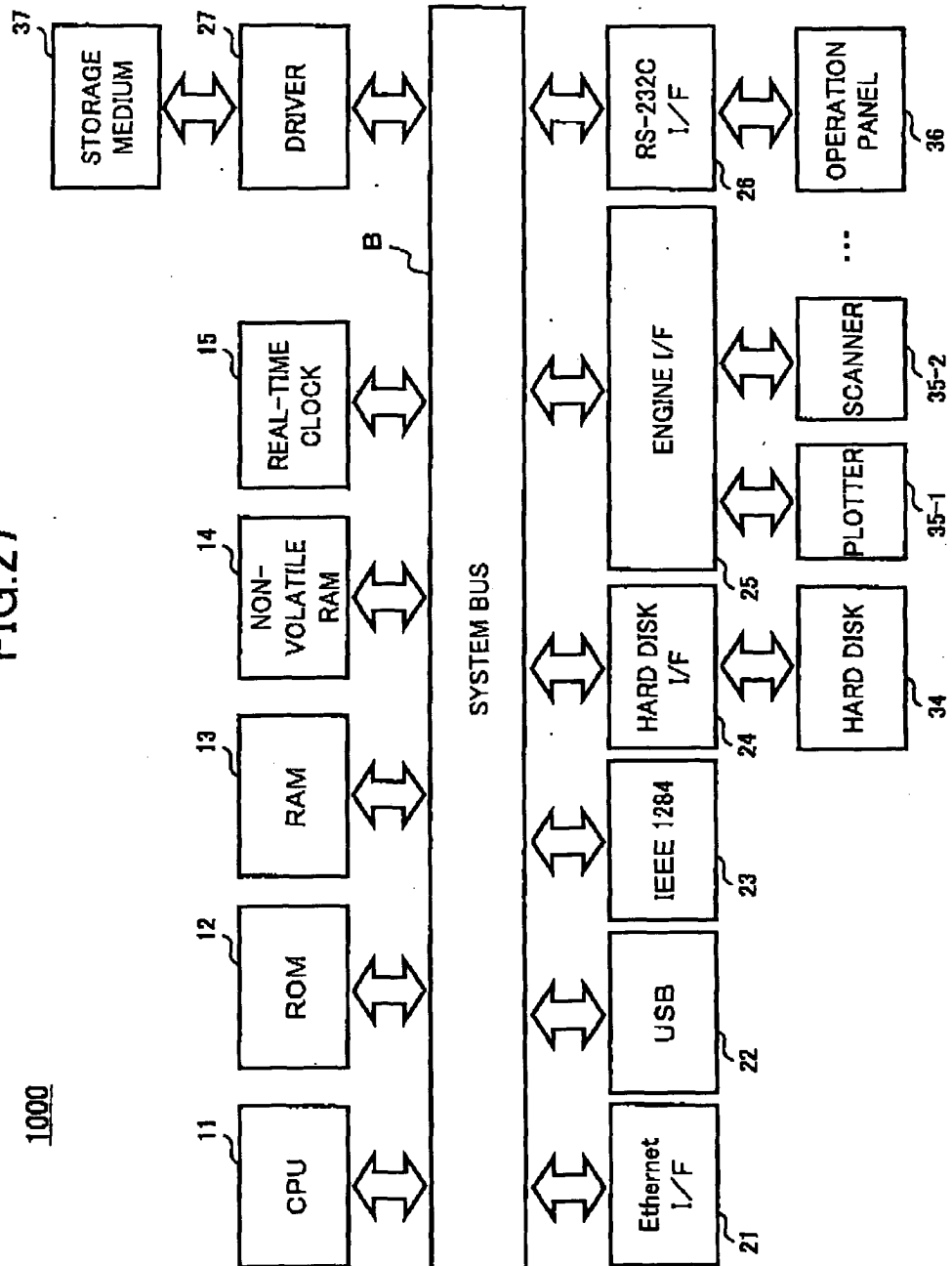


FIG.27



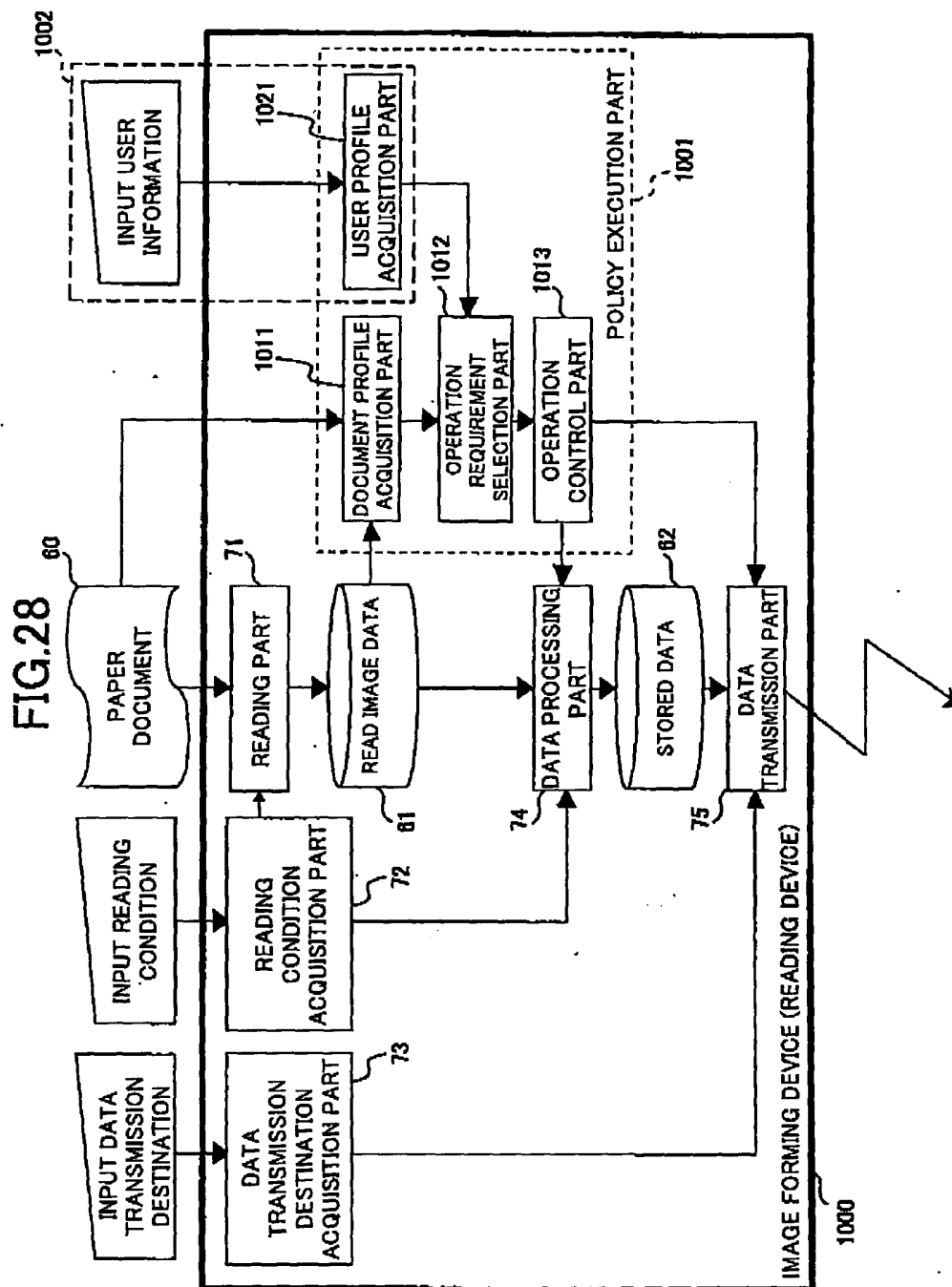


FIG.29

2100

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          <requirement>print_restriction</requirement>
          <requirement>trusted_channel</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>high</doc_security_level>
  <acl>
    <ace>
      <user_category>DOC-CATEGORY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>scan</name>
        <requirement>audit</requirement>
        <requirement>embed_trace_info</requirement>
      </operation>
    </ace>
  </acl>
</acc_rule>
</policy>
```

FIG.30

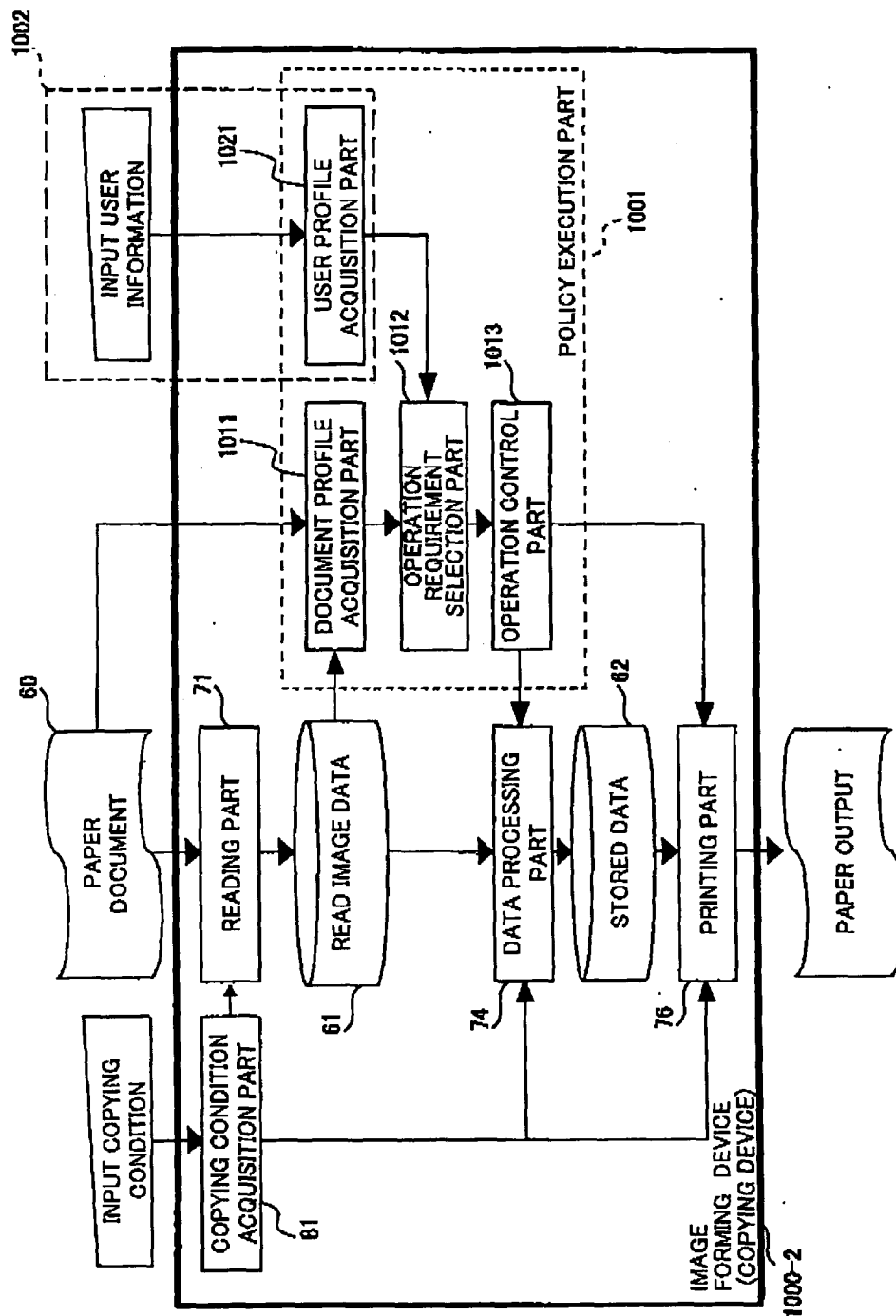
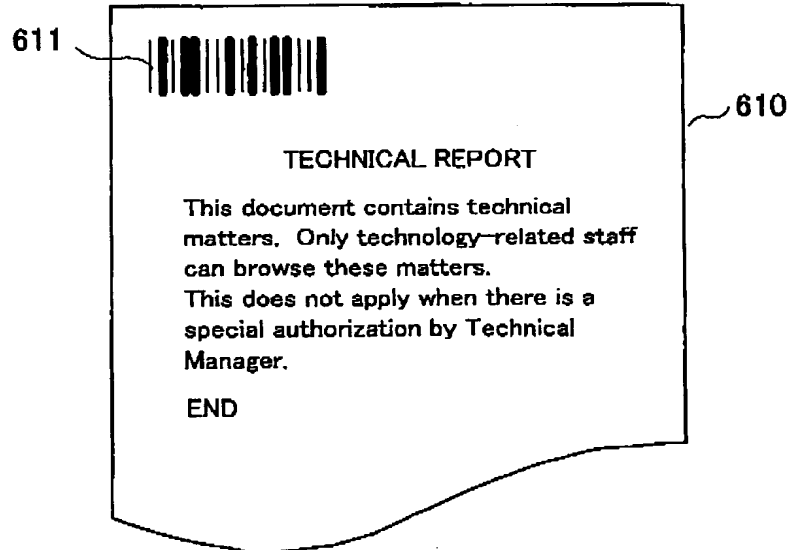


FIG.31



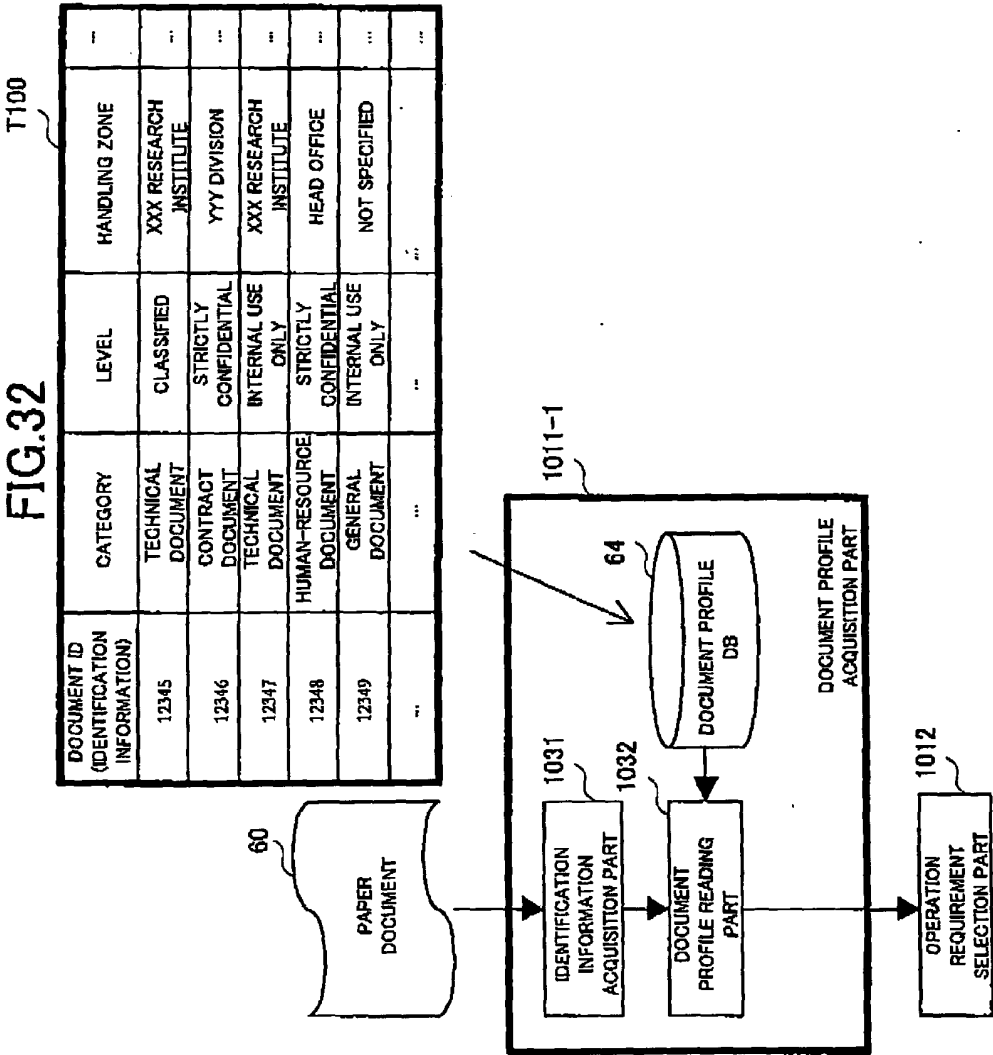


FIG.33

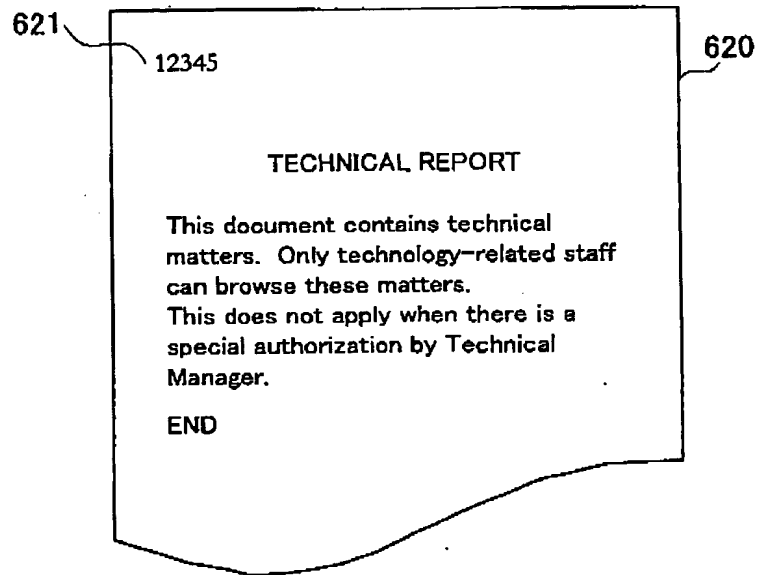


FIG. 34

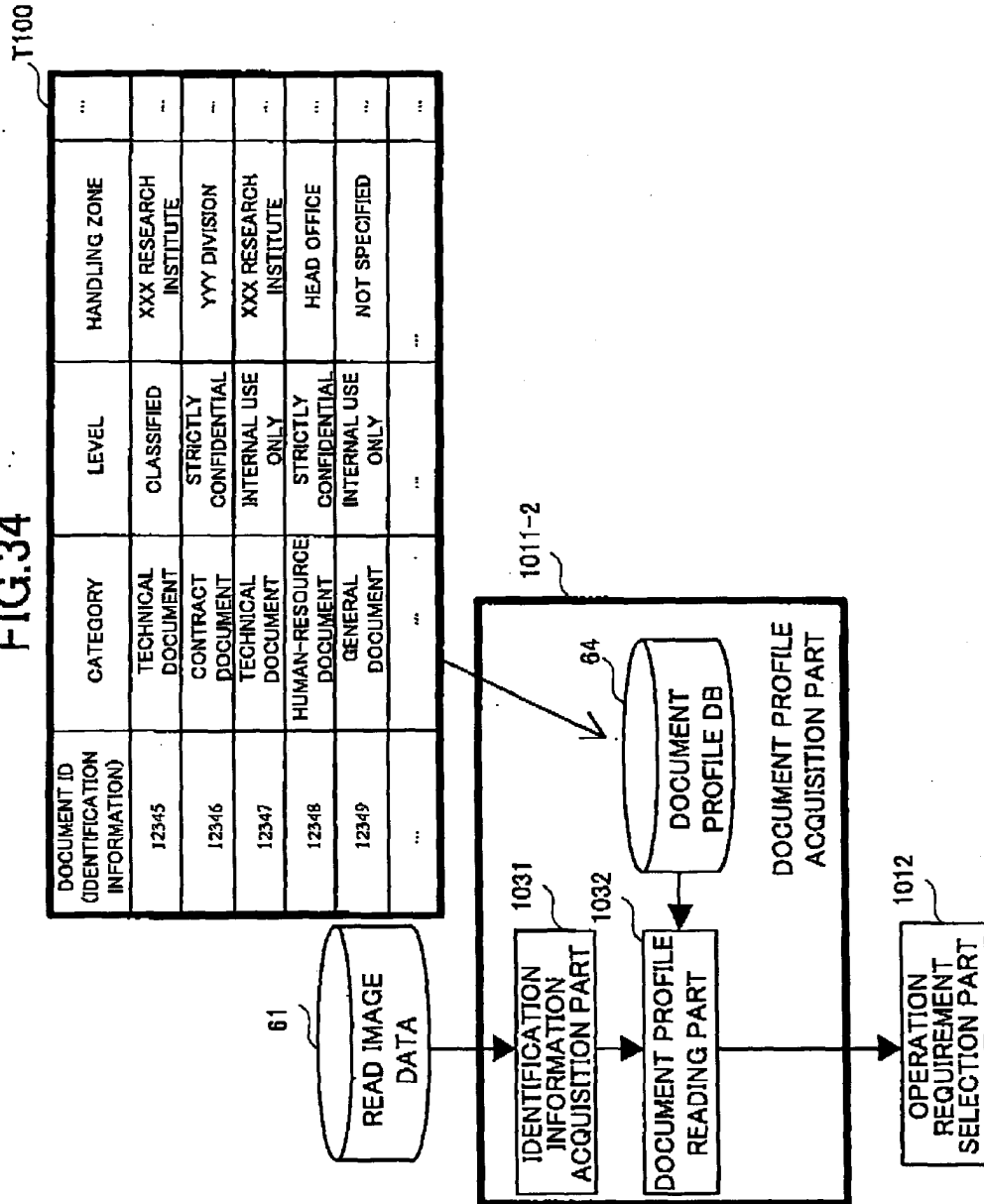


FIG.35

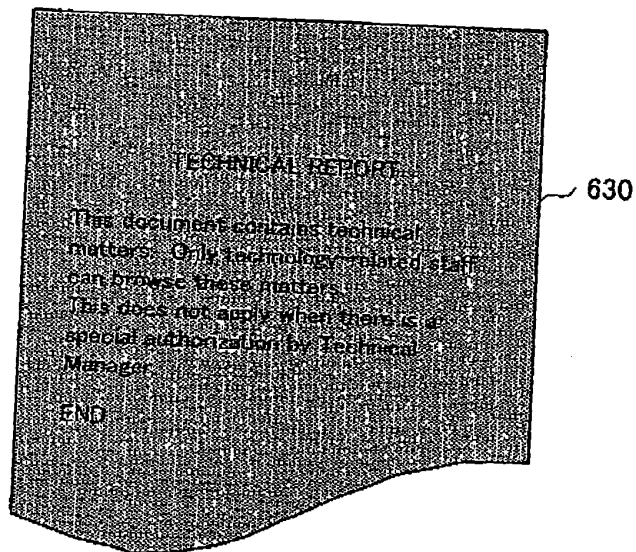


FIG.36

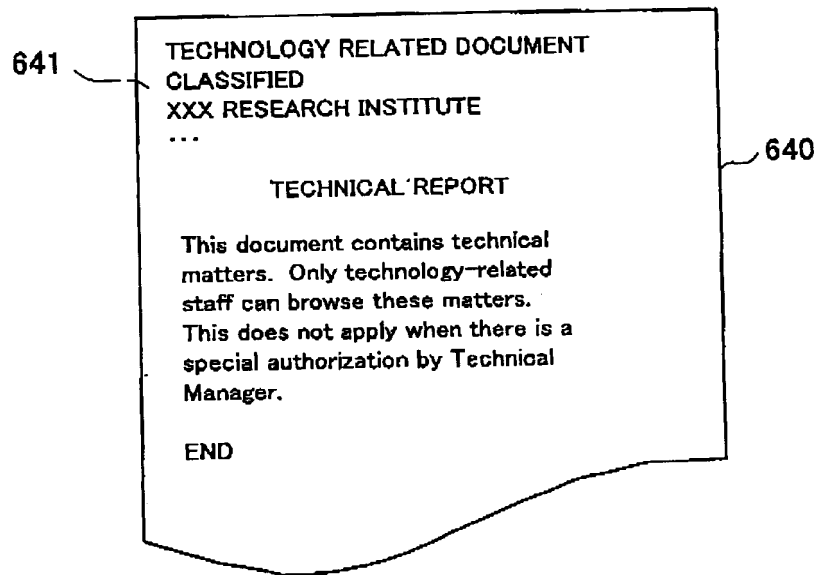


FIG.37

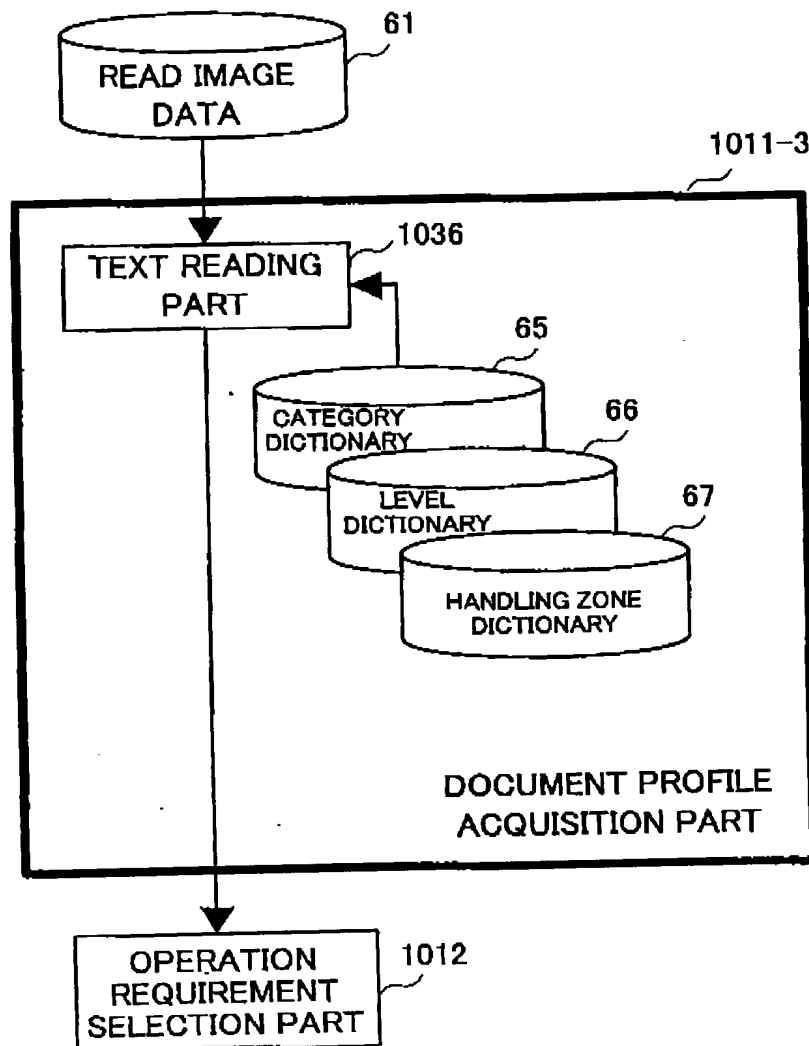


FIG.38

T200

USER ID	PASSWORD	CATEGORY	LEVEL	...
01234	%#2& D7soeb	TECHNICAL DIVISION	ADMINISTRATOR	...
01235	aova3&wh%bcfln	PRODUCTION DIVISION	EXTERNAL	...
01236	U#K5ccsaw7yc	TECHNICAL DIVISION	GENERAL	...
01237	IU)28Gtw?%	DIVISION HUMAN RESOURCES	ADMINISTRATOR	...
01238	# shjIwOadh#63	HEAD OFFICE	GENERAL	...
...

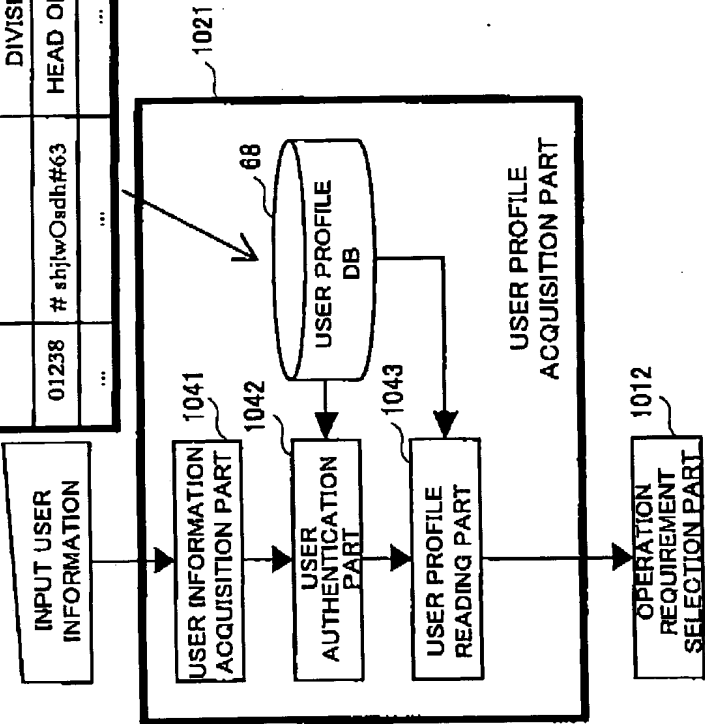


FIG.39

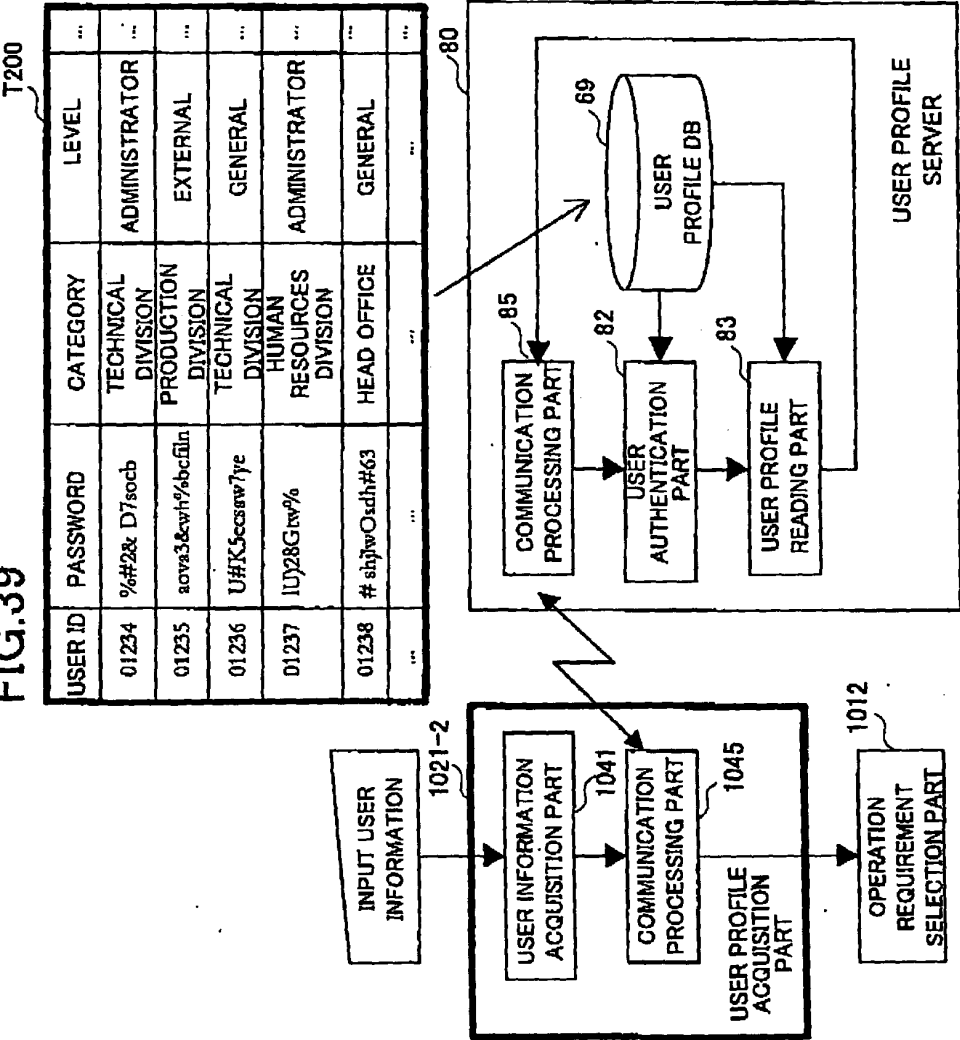


FIG.40

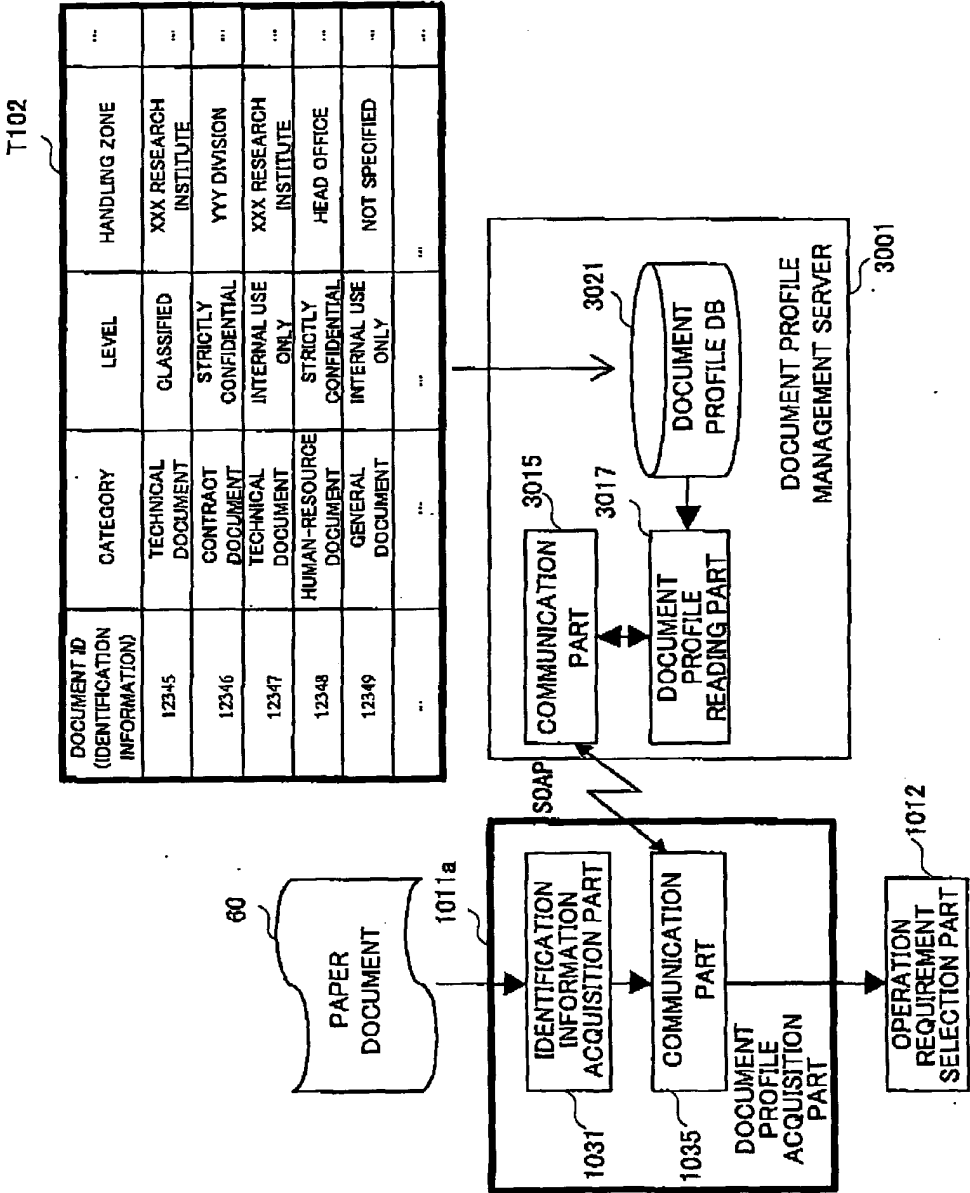


FIG.41

T102

DOCUMENT ID (IDENTIFICATION INFORMATION)	CATEGORY	LEVEL	HANDLING ZONE
12345	TECHNICAL DOCUMENT	CLASSIFIED	XXX RESEARCH INSTITUTE
12346	CONTRACT DOCUMENT	STRICTLY CONFIDENTIAL	YYY DIVISION
12347	TECHNICAL DOCUMENT	INTERNAL USE ONLY	XXX RESEARCH INSTITUTE
12348	HUMAN-RESOURCE DOCUMENT	STRICTLY CONFIDENTIAL	HEAD OFFICE
12349	GENERAL DOCUMENT	INTERNAL USE ONLY	NOT SPECIFIED
..

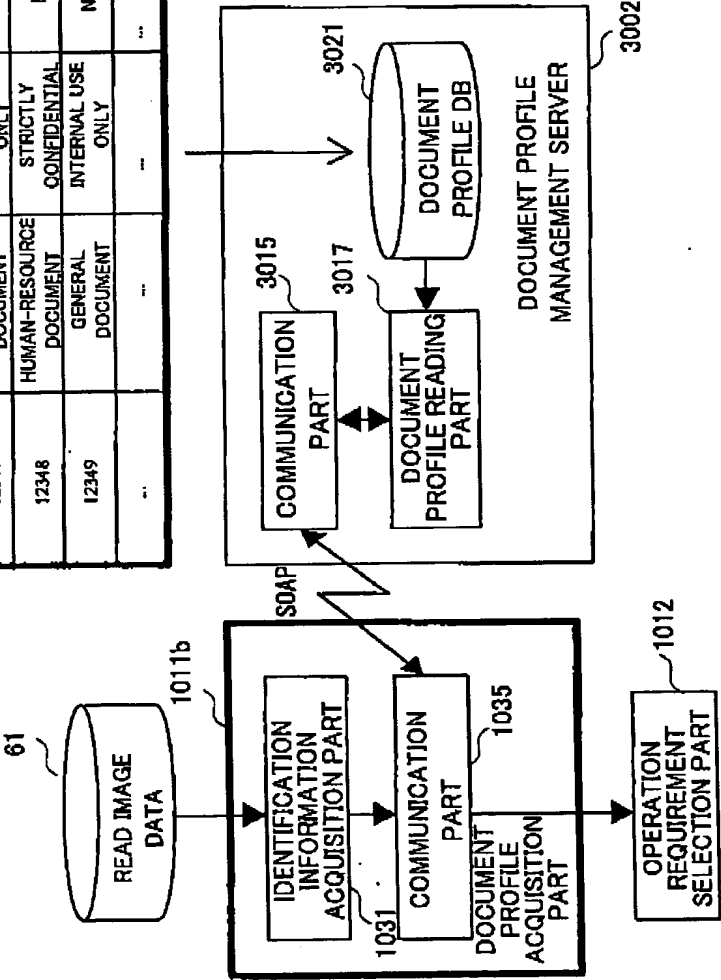
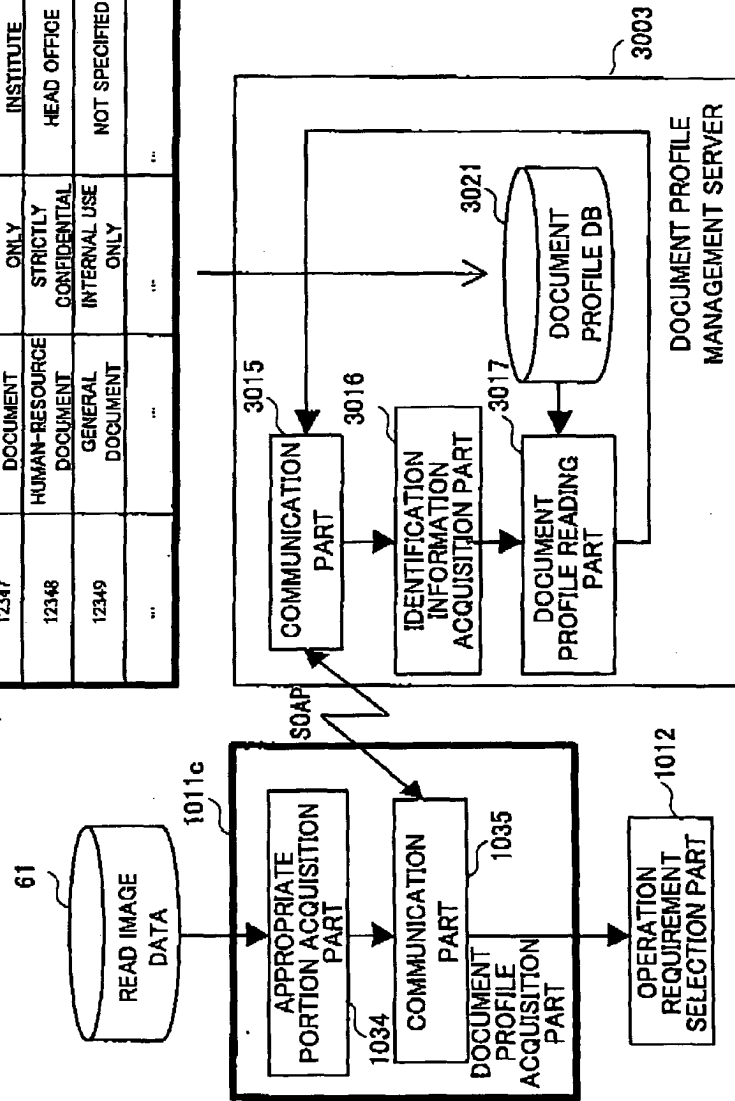


FIG.42

T102

DOCUMENT ID (IDENTIFICATION INFORMATION)	CATEGORY	LEVEL	HANDLING ZONE
12345	TECHNICAL DOCUMENT	CLASSIFIED	XXX RESEARCH INSTITUTE
12346	CONTRACT DOCUMENT	STRICTLY CONFIDENTIAL	YYY DIVISION
12347	TECHNICAL DOCUMENT	INTERNAL USE ONLY	XXX RESEARCH INSTITUTE
12348	HUMAN-RESOURCE DOCUMENT	STRICTLY CONFIDENTIAL	HEAD OFFICE
12349	GENERAL DOCUMENT	INTERNAL USE ONLY	NOT SPECIFIED
...



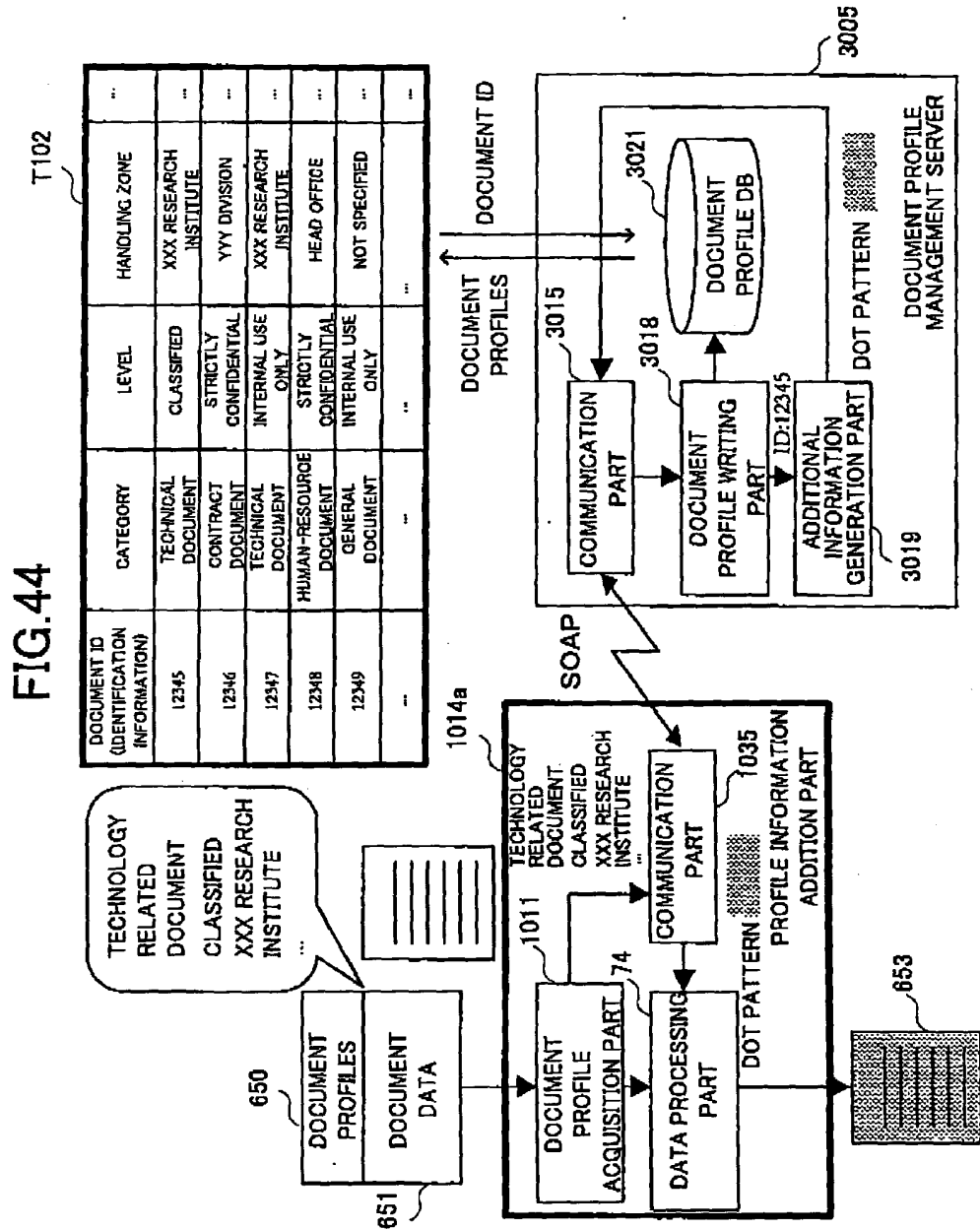


FIG.45

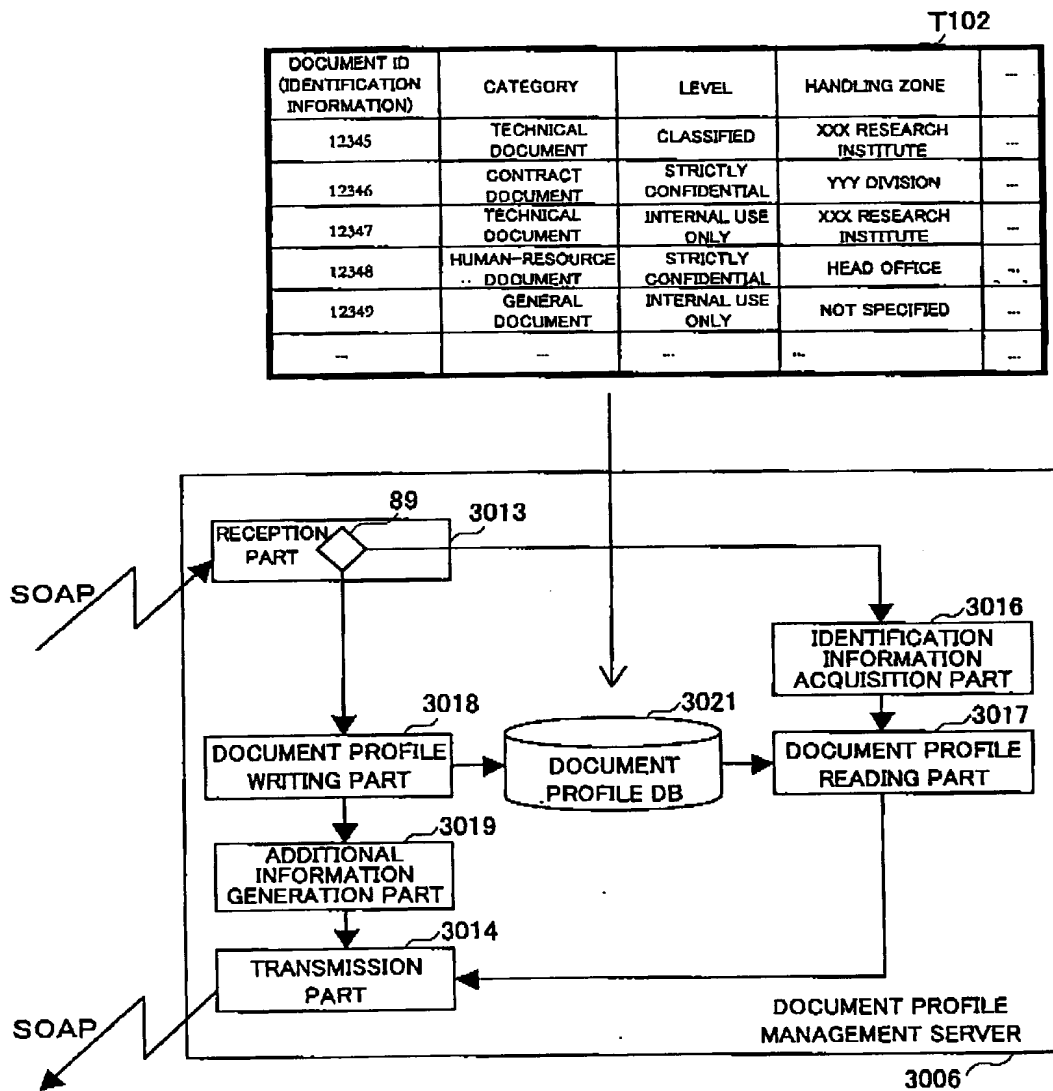


FIG.46

700

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:documentProfileRequest>
      <soapenv:encodingStyle=http://schemas.xmlsoap.org/soap/encoding/
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/docprofs">
        <ticket>
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
          ANnQexdYxm/Fy7T1xwB83qXEBUjcwgeVhCYu/kdcIDTcBstavhkyJtps=
        </ticket>
        <docInfo xsi:type="ns1:DocInfo"
          <secId xsi:type="xsd:string">12345</secId>
          <image xsi:type="soapenc:base64"></image>
          <imageType xsi:type="xsd:string" xsi:nil="true"/>
          <sizeX xsi:type="xsd:int" xsi:nil="true"/>
          <sizeY xsi:type="xsd:int" xsi:nil="true"/>
          <bitPerPixel xsi:type="xsd:int" xsi:nil="true"/>
        </docInfo>
      </ns1:documentProfileRequest>
    </soapenv:Body>
  </soapenv:Envelope>
```

701

703

FIG.47

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:documentProfileRequest 711
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
          AMcQaxdYxm/FyT1xwB83qXEBUicwgeVhOCYu/kdc10TcBtavhkyJtps=
        </ticket>
        <docInfo xsi:type="ns1:DocInfo"
          <docId xsi:type="xsd:string" xsi:nil="true"/>
          <image xsi:type="soapenc:base64">
            Electronic Image Data
          </image>
          <imageType xsi:type="xsd:string">BMP</imageType>
          <sizeX xsi:type="xsd:int">256</sizeX>
          <sizeY xsi:type="xsd:int">256</sizeY>
          <bitPerPixel xsi:type="xsd:int">8</bitPerPixel>
        </docInfo>
      </ns1:documentProfileRequest >
    </soapenv:Body>
  </soapenv:Envelope>

```

710

713

FIG.48

720

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:documentProfileResponse 721
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <docProfs xsi:type="ns1:DocProfs" 724
          <secId xsi:type="xsd:string">12345</secId> 725
          <category xsi:type="xsd:string">technical_doc</category> 726
          <level xsi:type="xsd:string">High</level> 727
          <zone xsi:type="xsd:string">99.99.0.0</zone>
        </docProfs>
      </ns1:documentProfileResponse>
    </soapenv:Body>
  </soapenv:Envelope>
```

FIG.49

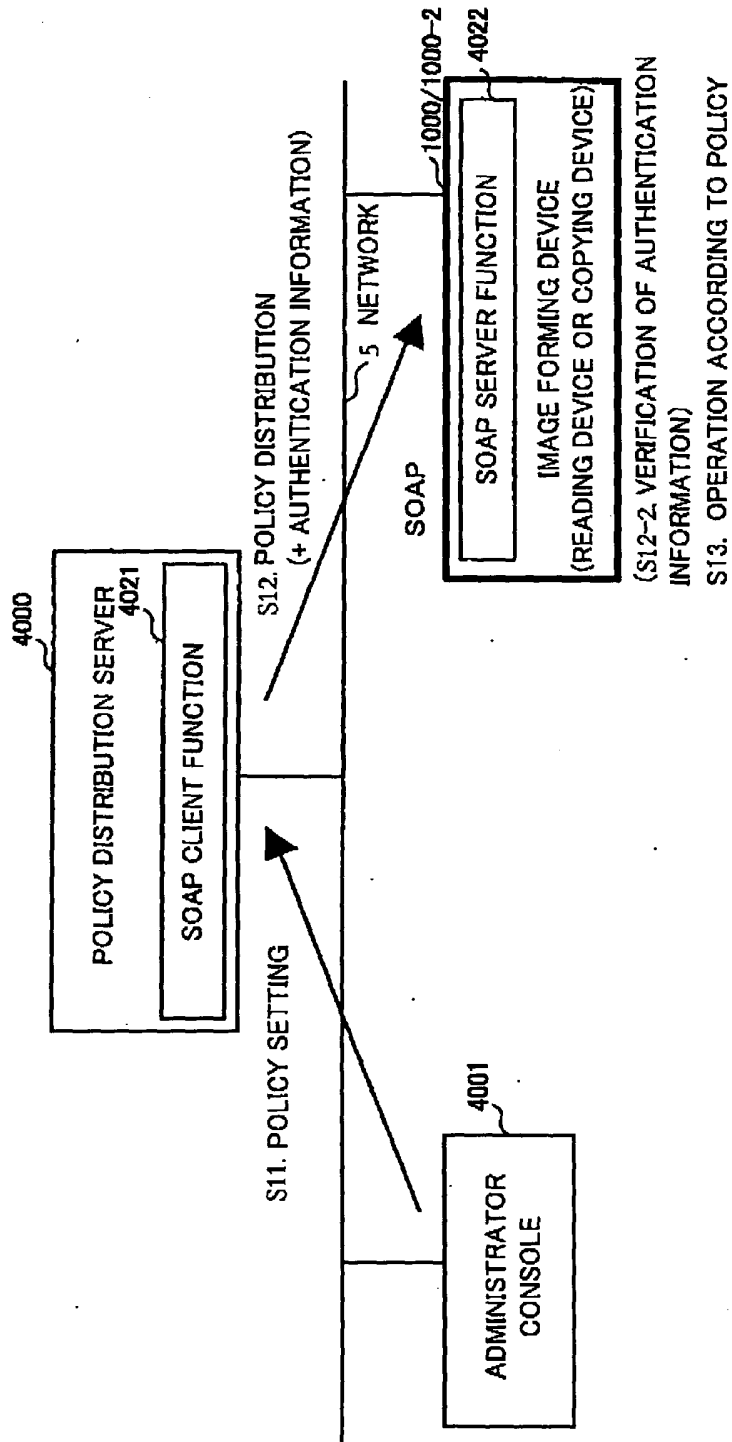


FIG.50

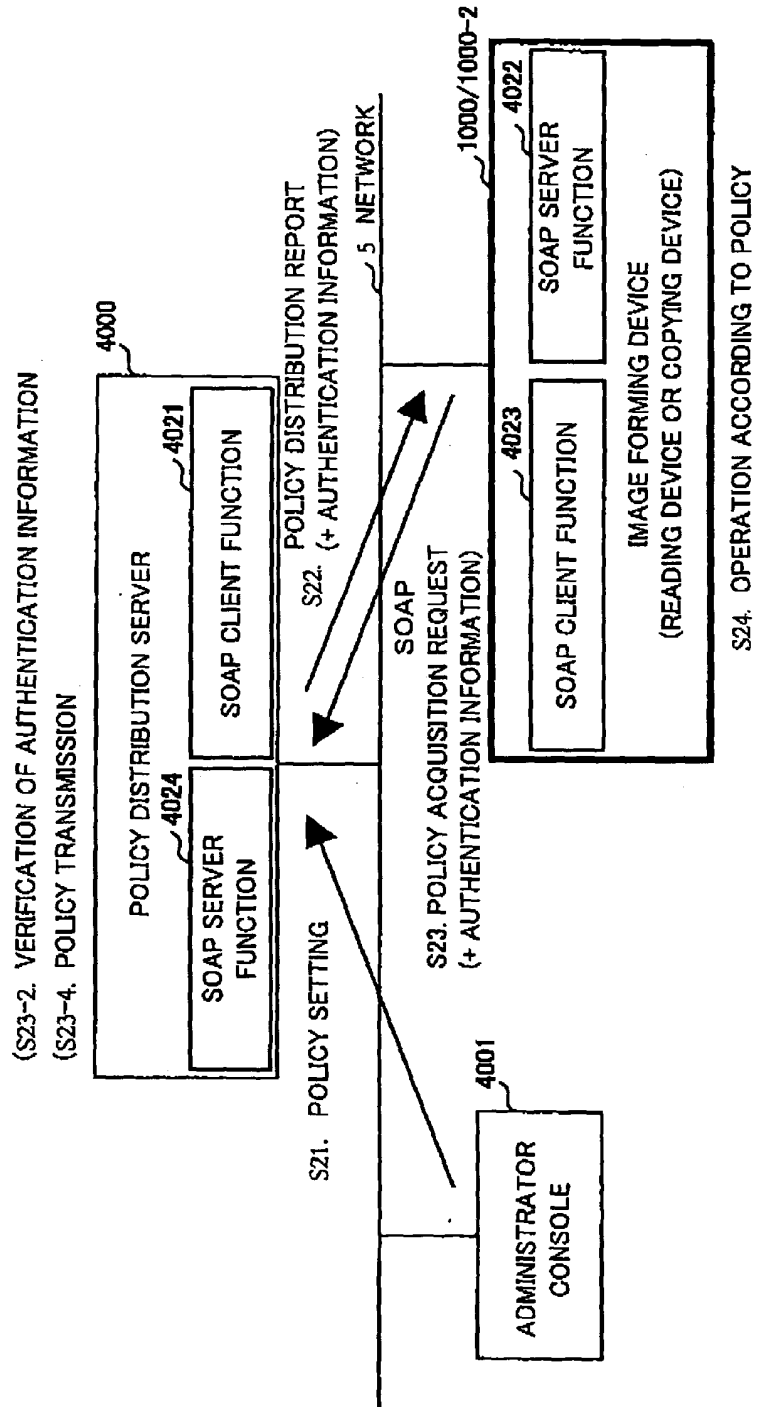


FIG.51

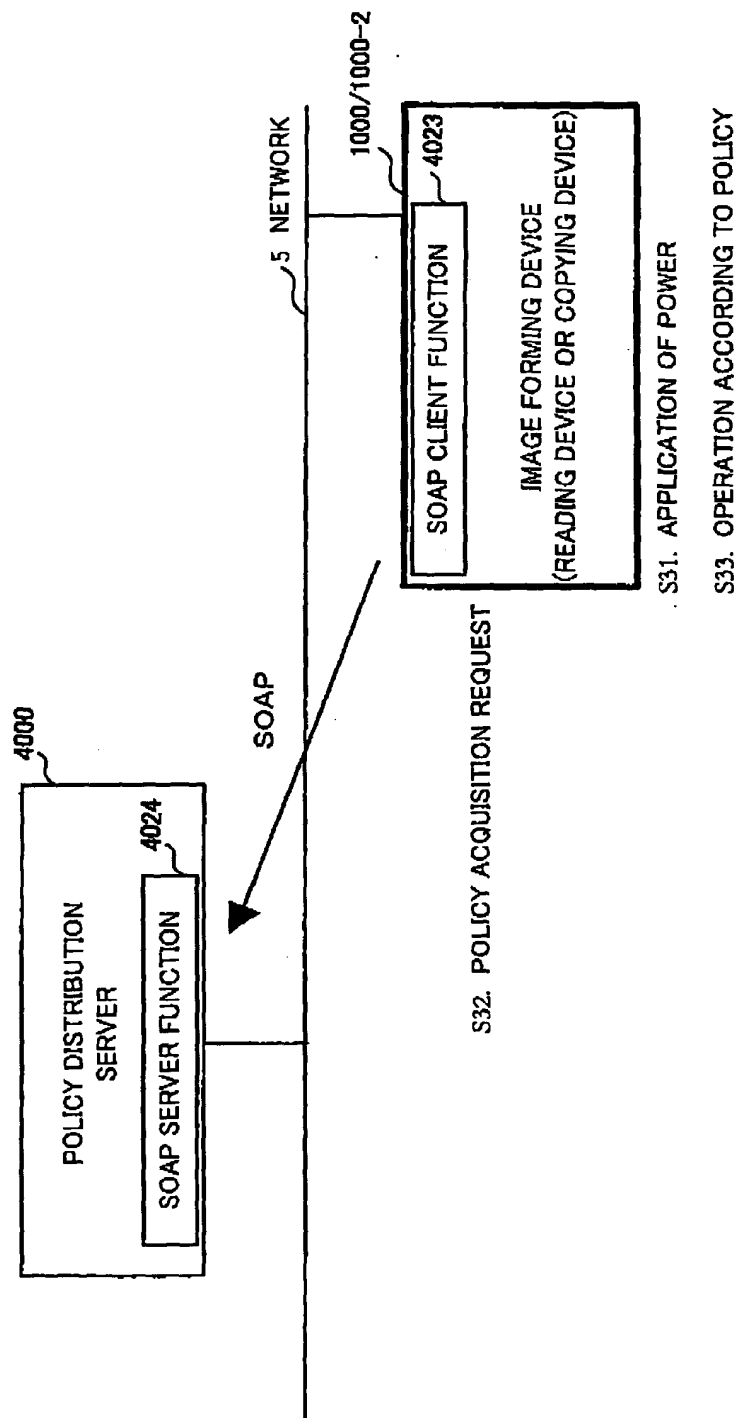


FIG.52

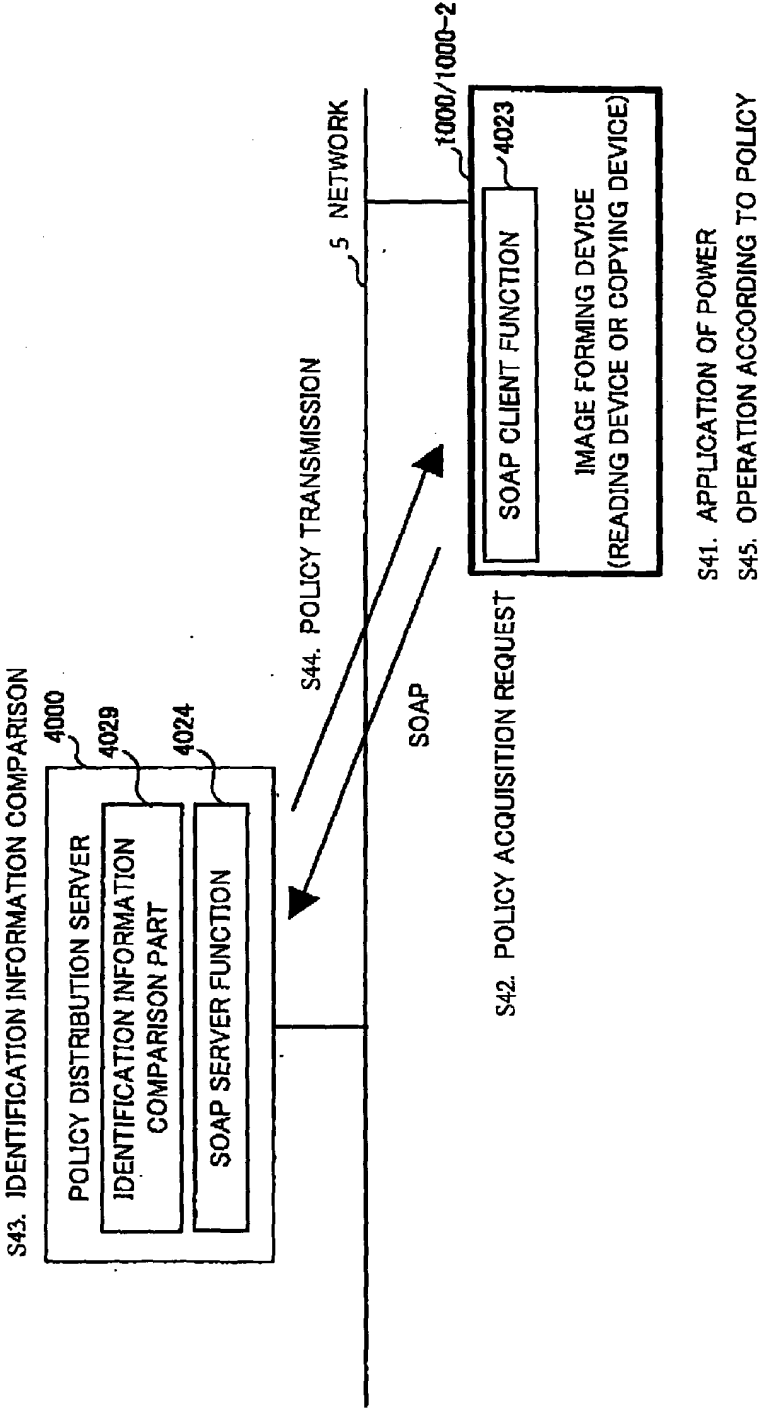


FIG.53

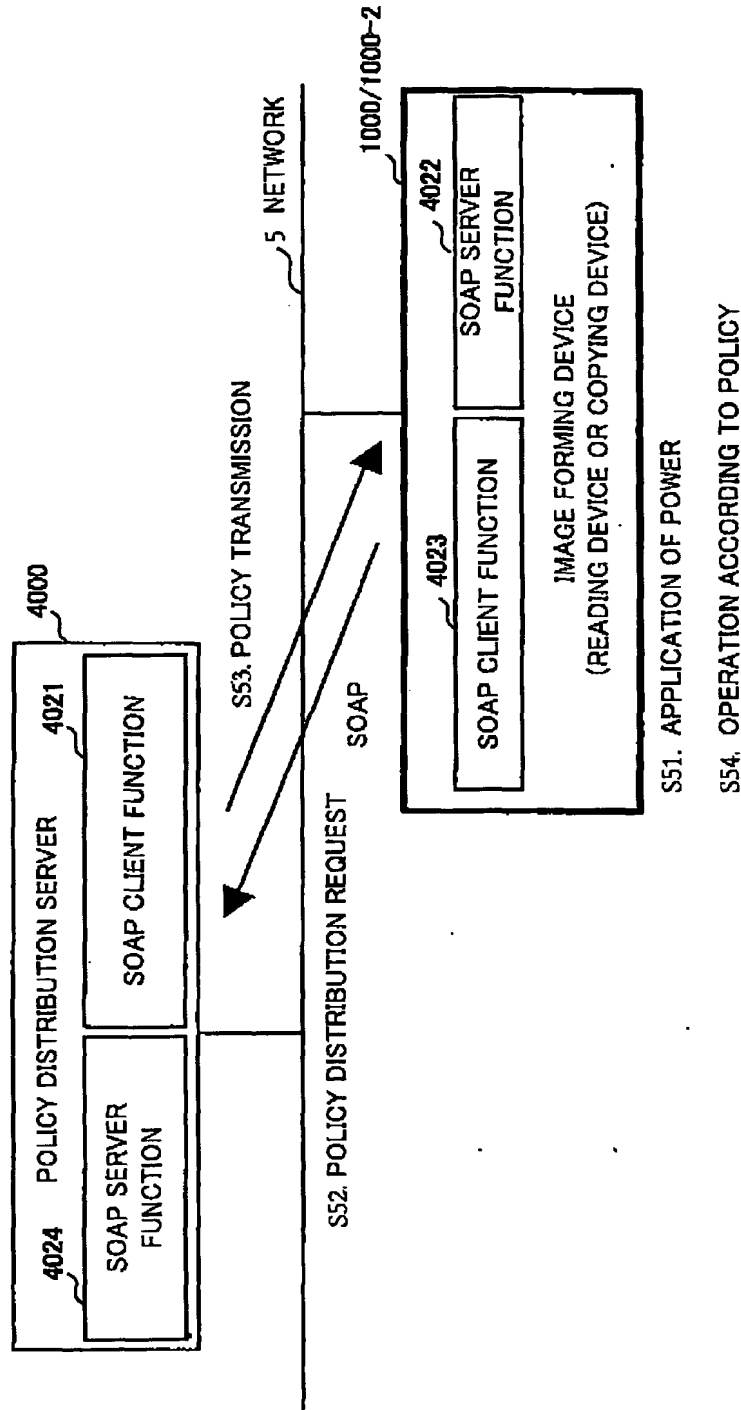


FIG. 54

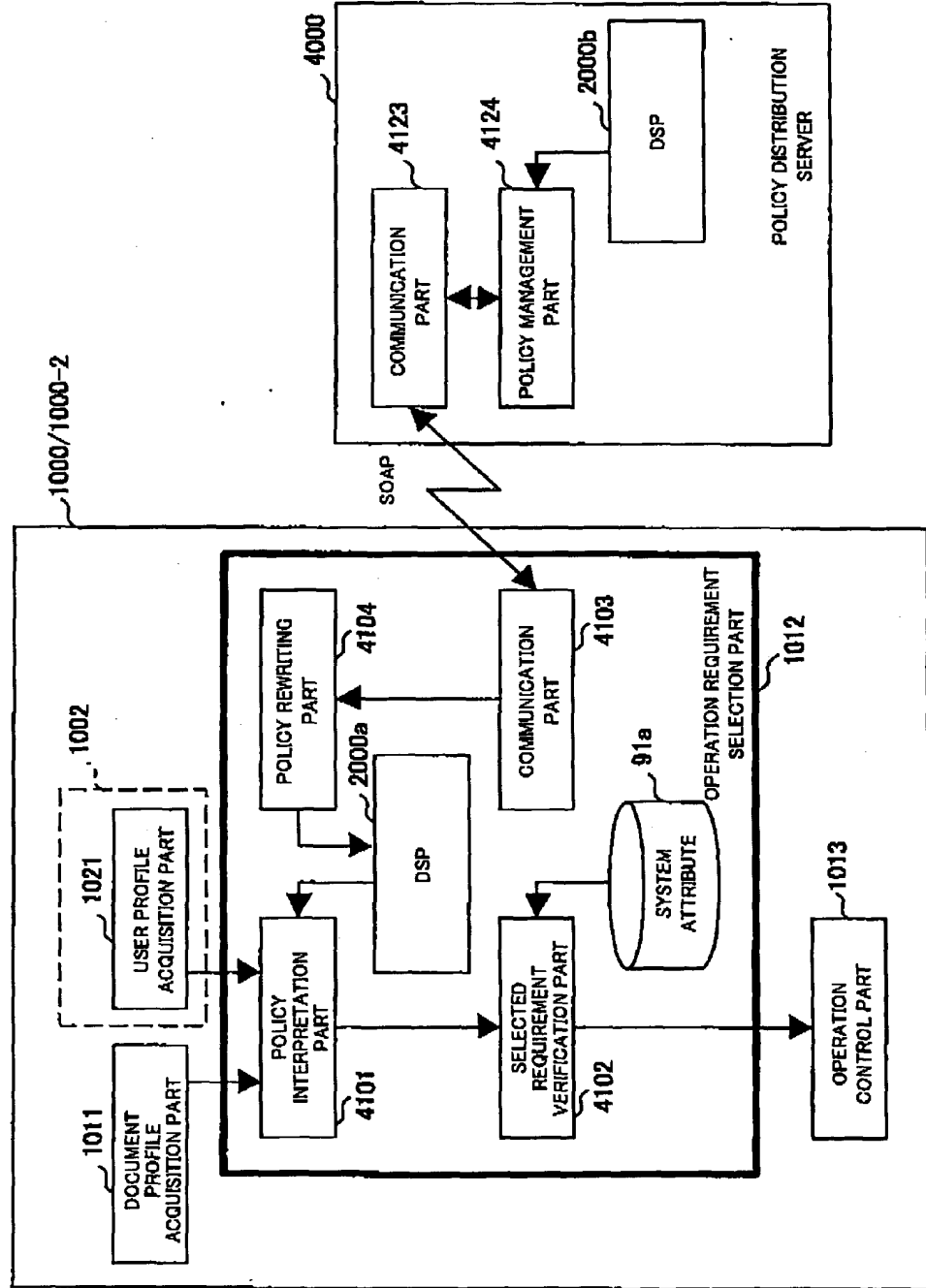


FIG.55

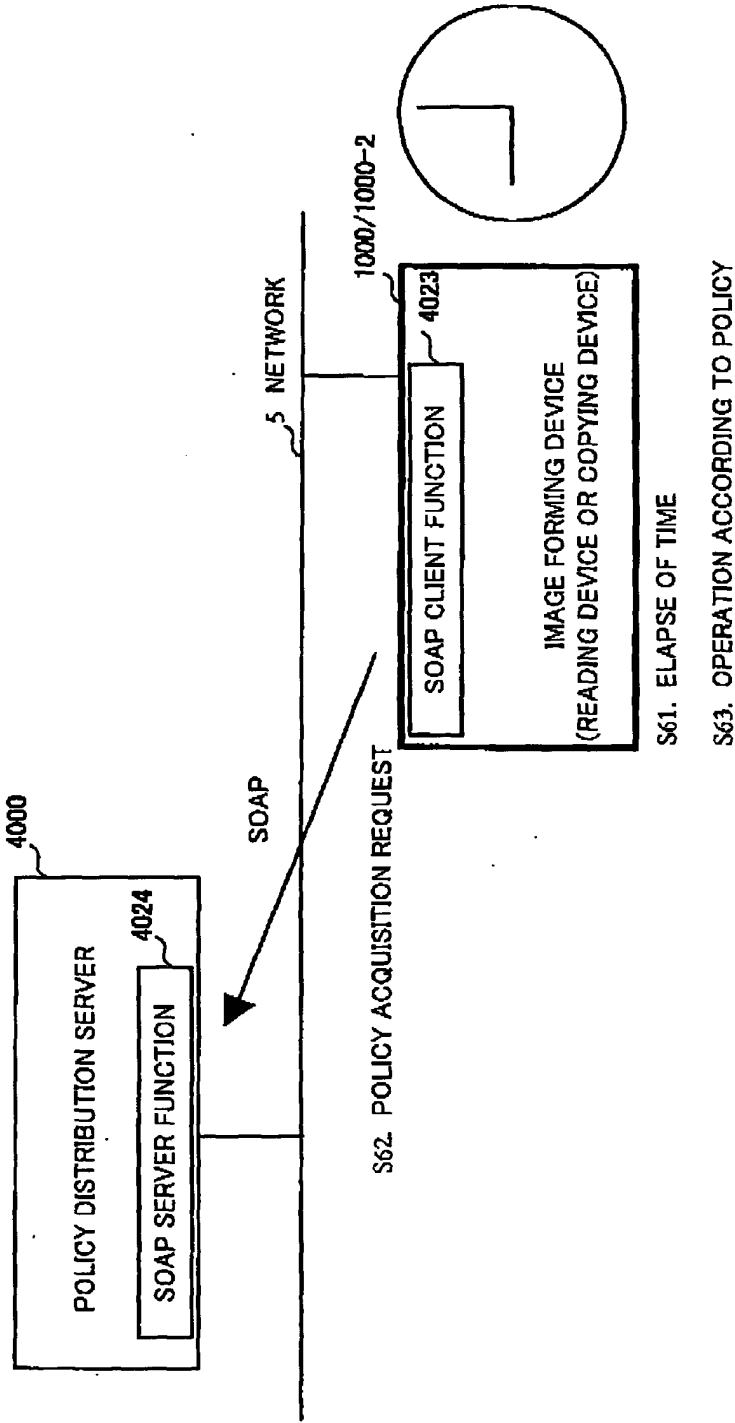


FIG.56

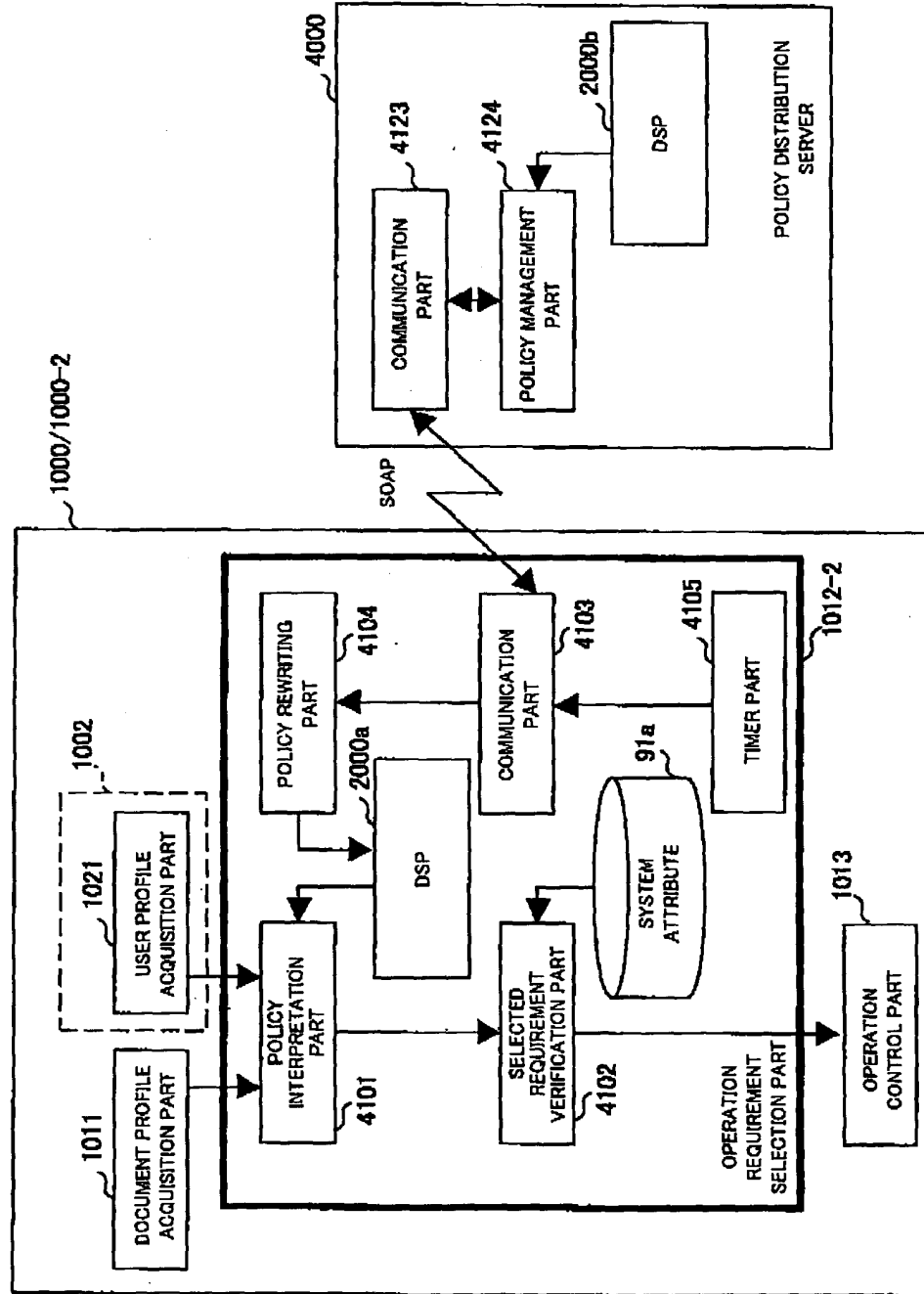


FIG.57

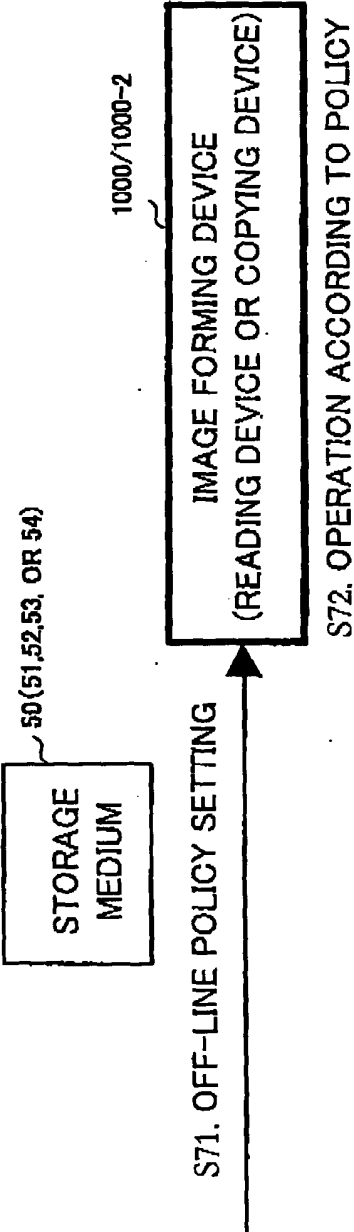


FIG.58

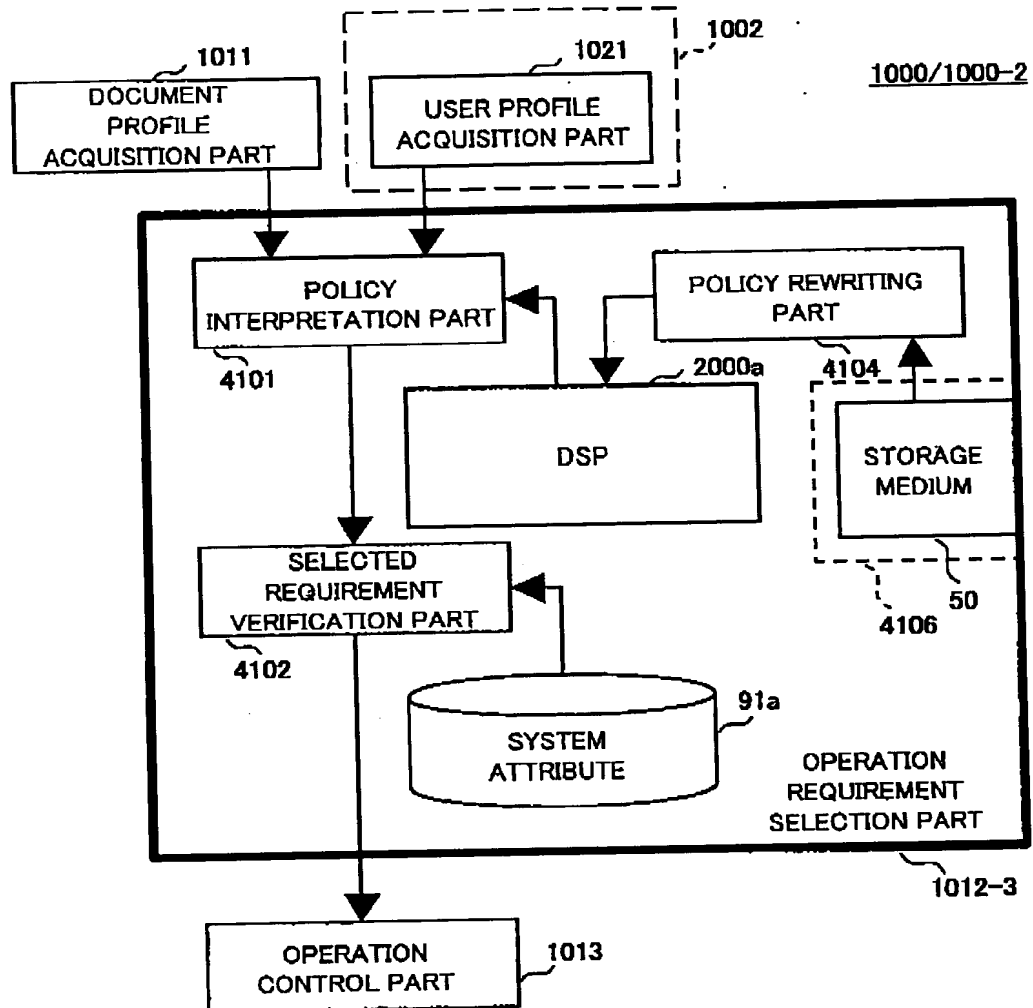


FIG.59

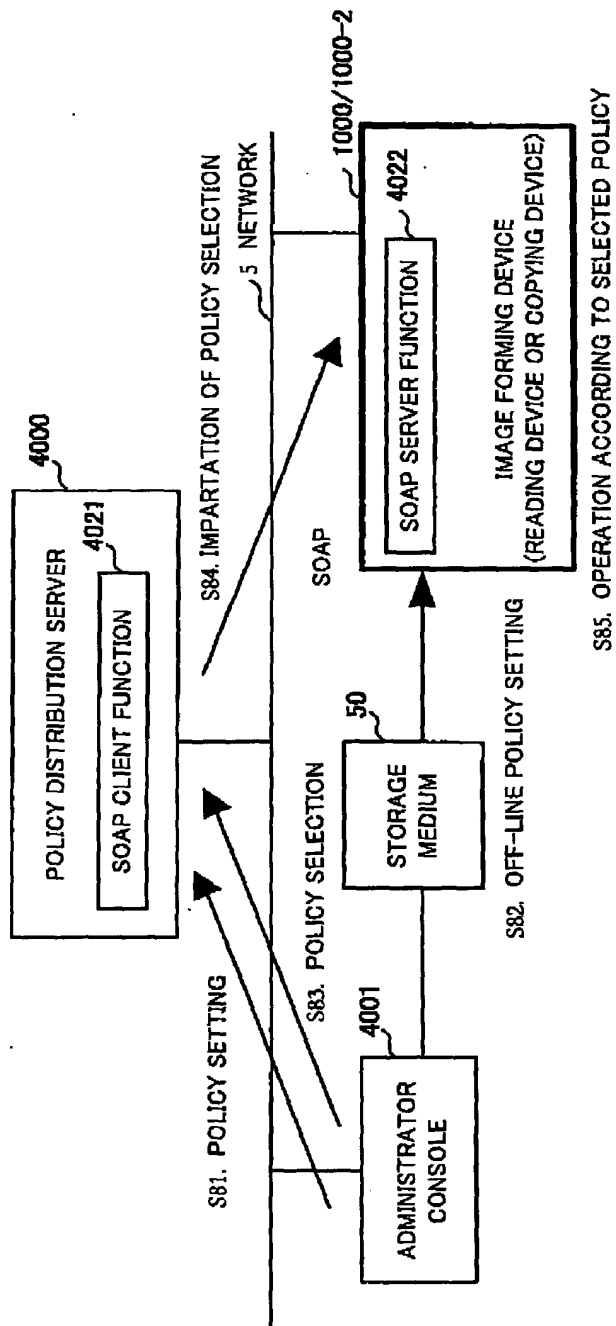


FIG. 60

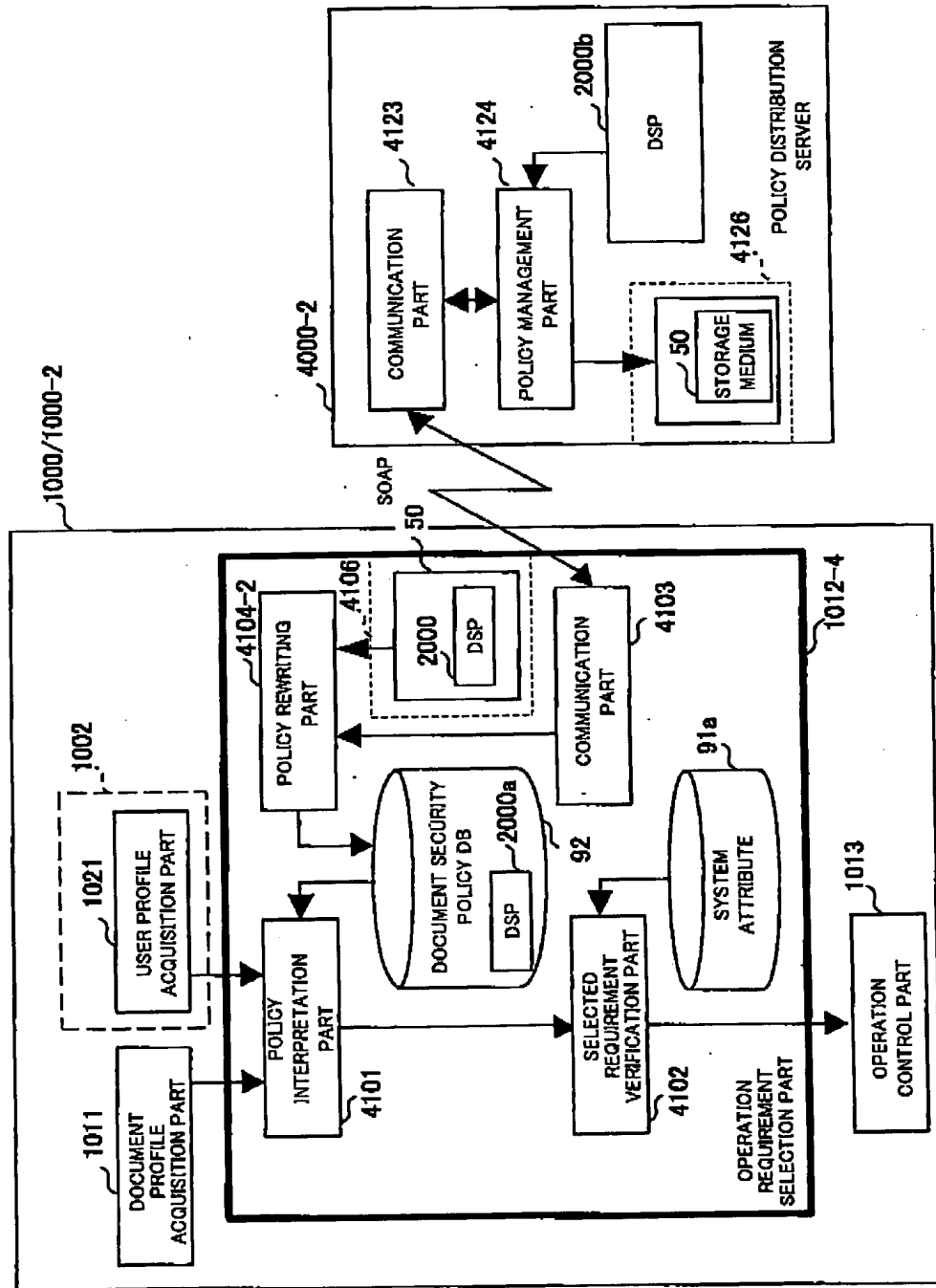


FIG. 61

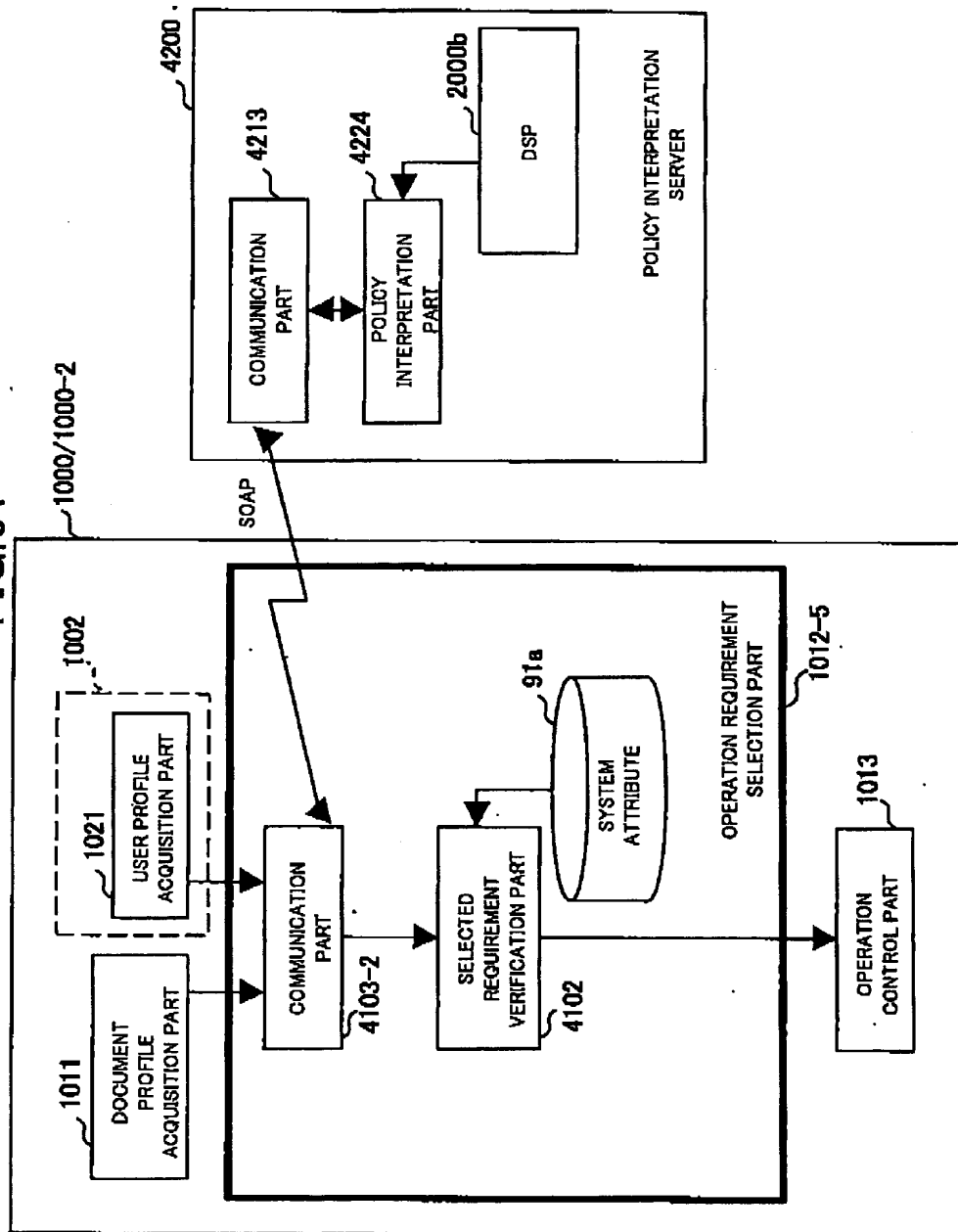


FIG.62

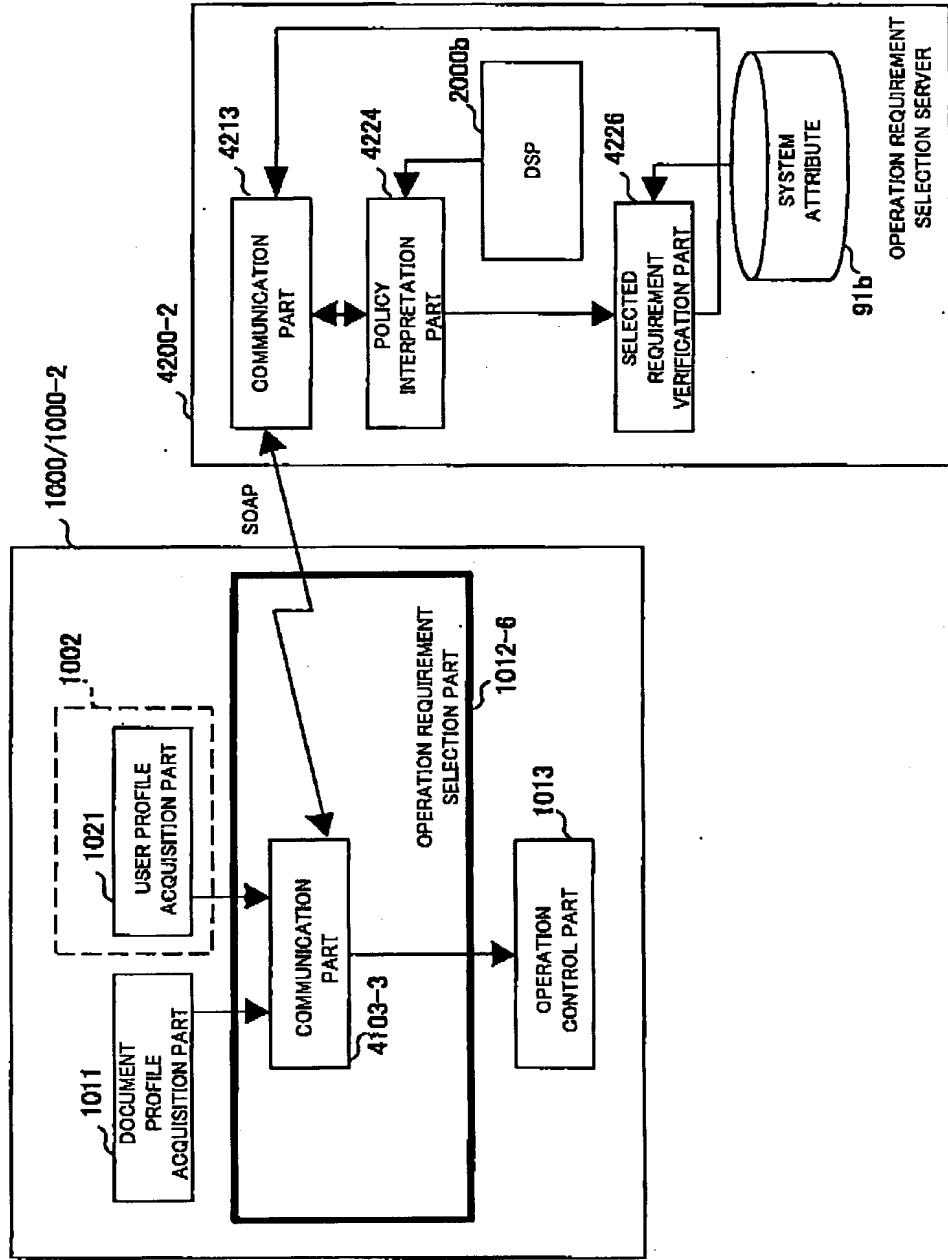


FIG.63

91a

OPERATION CONDITION	SUPPORT
RECORDING LOG	O
RECORDING IMAGE LOG	x
PRINTING CONFIDENTIALITY LABEL	O
PRINTING OPERATOR LABEL	O
PRINTING IDENTIFICATION BAR CODE	x
PRINTING IDENTIFICATION PATTERN	O
...	...

FIG.64

91b

OPERATION CONDITION	DEVICE 01	DEVICE 02	DEVICE 03	DEVICE 04	...
RECORDING LOG	○	○	○	○	
RECORDING IMAGE LOG	x	x	○	○	
PRINTING CONFIDENTIALITY LABEL	○	○	○	○	
PRINTING OPERATOR LABEL	○	x	○	x	
PRINTING IDENTIFICATION BAR CODE	x	x	○	x	
PRINTING IDENTIFICATION PATTERN	○	x	○	x	
...

FIG.65

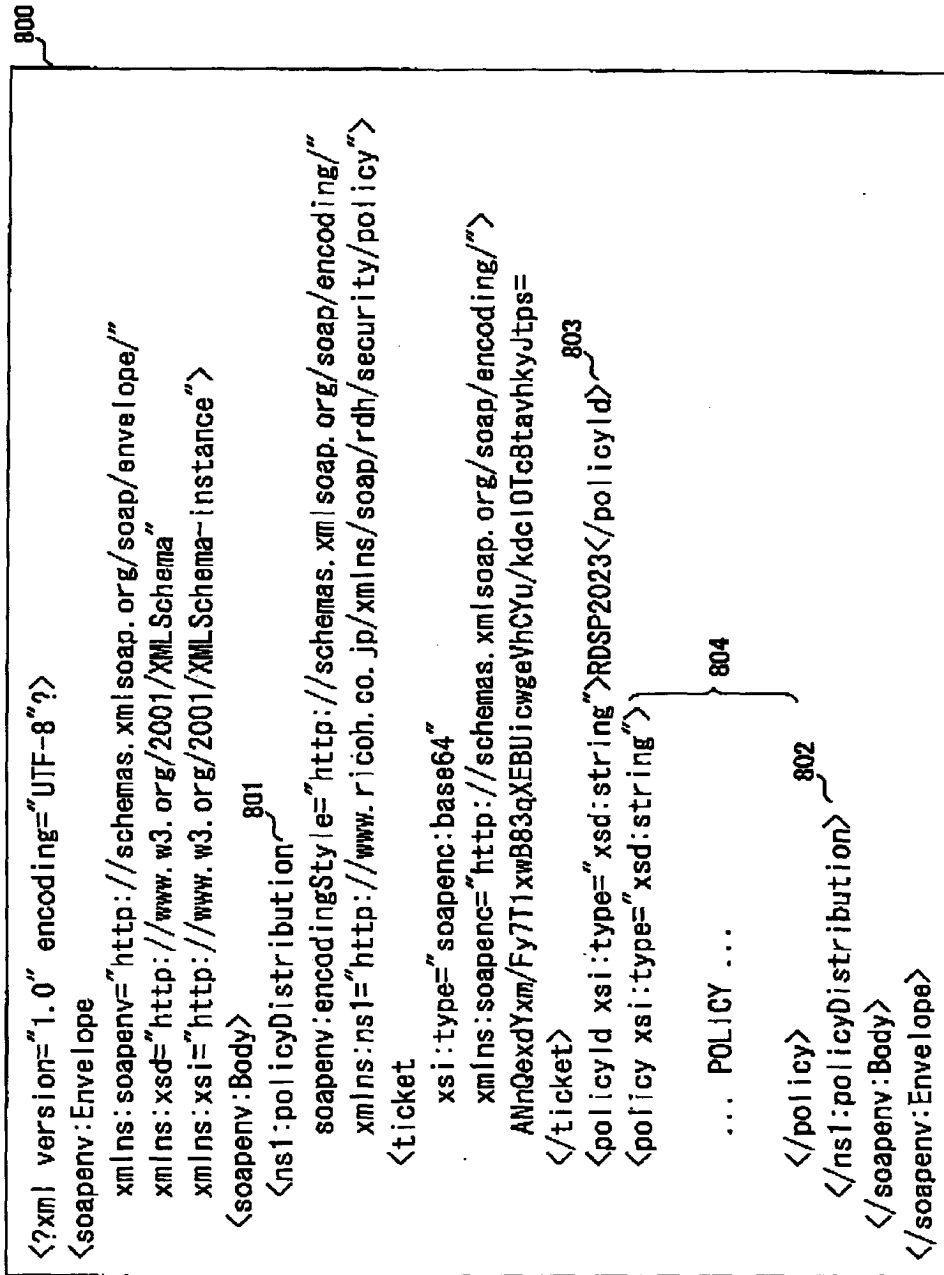


FIG.66

810

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistributionResponse 811
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <result xsi:type="xsd:boolean">true</result> 813
    </ns1:policyDistributionResponse> 812
  </soapenv:Body>
</soapenv:Envelope>
```

FIG.67

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistributionReport ~ 821
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
          ANnQexdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdc10TcBtavhkyJtps=
        </ticket>
        <policyId xsi:type="xsd:string">RDSP2023</policyId> ~ 823
      </ns1:policyDistributionReport> ~ 822
    </soapenv:Body>
  </soapenv:Envelope>

```

820

FIG.68

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyRequest 831
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
        <ticket
          xsi:type="soapenc:base64"
          xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
            ANn0exdYxm/shuqjIKsy73kahqw520iUsJqIhHKJ/kdc10Tc8tavhkyJtps=
          </ticket>
          <policyId xsi:type="xsd:string">RDSP2023</policyId> 833
        </ns1:policyRequest> 832
      </soapenv:Body>
    </soapenv:Envelope>
```

830

FIG.69

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistribution 841
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <ticket
        xsi:type="soapenc:base64"
        xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
      </ticket>
      <policyId xsi:type="xsd:string">RDSP2023</policyId> 843
      <policy xsi:type="xsd:string">
        ... POLICY...
      </policy>
    </ns1:policyDistribution> 842
  </soapenv:Body>
</soapenv:Envelope>
```

840

FIG.70

850

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyDistributionRequest ~
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <policyId xsi:type="xsd:string">RDSP2023</policyId> ~
      </ns1:policyDistributionRequest> ~
    </soapenv:Body>
  </soapenv:Envelope>

```

851

853

852

FIG. 71

860

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:policyChangeRequest 861
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
      <ticket
        xsi:type="soapenc:base64"
        xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
        ANn0exdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdc10Tc8tavhkyJtps=
      </ticket>
      <policyId xsi:type="xsd:string">RDSP2023</policyId> 863
    </ns1:policyChangeRequest> 862
  </soapenv:Body>
</soapenv:Envelope>
```

FIG. 72

870

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:isAllowed
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/security/sectk">
      <userTicketInfo
        xsi:type="ns2:authTicketInfo"
        xmlns:ns2="http://www.ricoh.co.jp/xmlns/schema/uaauthentication"
      >
        <targets>
          <expireDate xsi:type="xsd:dateTime">
            2003-04-02T11:29:48.796Z
          </expireDate>
          <userInfo xsi:type="ns2:principal">
            <id xsi:type="xsd:string">U:Notes:CN=Atsuhisa Saitoh, OU=R, O=RRR/id>
            <principalType xsi:type="xsd:string">user</principalType>
            <userSpace xsi:type="xsd:string">Notes</userSpace>
            <domainName xsi:type="xsd:string">RGroup</domainName>
            <name xsi:type="xsd:string">Atsuhisa Saitoh/R/RRR/name>
          </userInfo>
        </targets>
      </userTicketInfo>
    </ns1:isAllowed>
  </soapenv:Body>
</soapenv:Envelope>
```

871

FIG.73

```
<groupInfo
  xsi:type="soapenc:Array"
  soapenc:arrayType="ns2:principal[1]"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
</item>
<id xsi:type="xsd:string">G:Notes:CN=PBDS_USERS</id>
<principalType xsi:type="xsd:string">group</principalType>
<userSpace xsi:type="xsd:string">Notes</userSpace>
<domainName xsi:type="xsd:string">RGroup</domainName>
<name xsi:type="xsd:string">PBDS_USERS</name>
</item>
</groupInfo> 874
</userTicketInfo>
<docInfo xsi:type="ns1:DocInfo"
  category xsi:type="xsd:string">Technical_doc</category> 882
  level xsi:type="xsd:string">High</level> 883
  zone xsi:type="xsd:string">99.99.99</zone> 884
</docInfo>
<accessInfo
  xsi:type="ns3:AccessInfo"
  xmlns:ns3="http://www.rrr.co.jp/xmlns/schema/security/policy"
  operation xsi:type="xsd:string">COPY</operation> 886
</accessInfo>
</ns1:isAllowed> 872
</soapenv:Body>
</soapenv:Envelope>
```

FIG.74

890

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:isAllowedResponse 891
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/seck">
        <isAllowedReturn
          xsi:type="ns2:DecisionInfoEx"
          xmlns:ns2="http://www.ricoh.co.jp/xmlns/schema/rdh/security/seck">
            <allowed xsi:type="xsd:boolean">true</allowed> 895
          <requirements
            { 896
              xsi:type="soapenc:Array"
              soapenc:arrayType="ns3:Requirement[1]"
              xmlns:ns3="http://www.ricoh.co.jp/xmlns/schema/rdh/security/policy"
              xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
            }
            <item>
              <requirement xsi:type="xsd:string">audit</requirement> 897
            </item>
          </requirements>
        </isAllowedReturn> 892
      </ns1:isAllowedResponse>
    </soapenv:Body>
  </soapenv:Envelope>

```

FIG.75

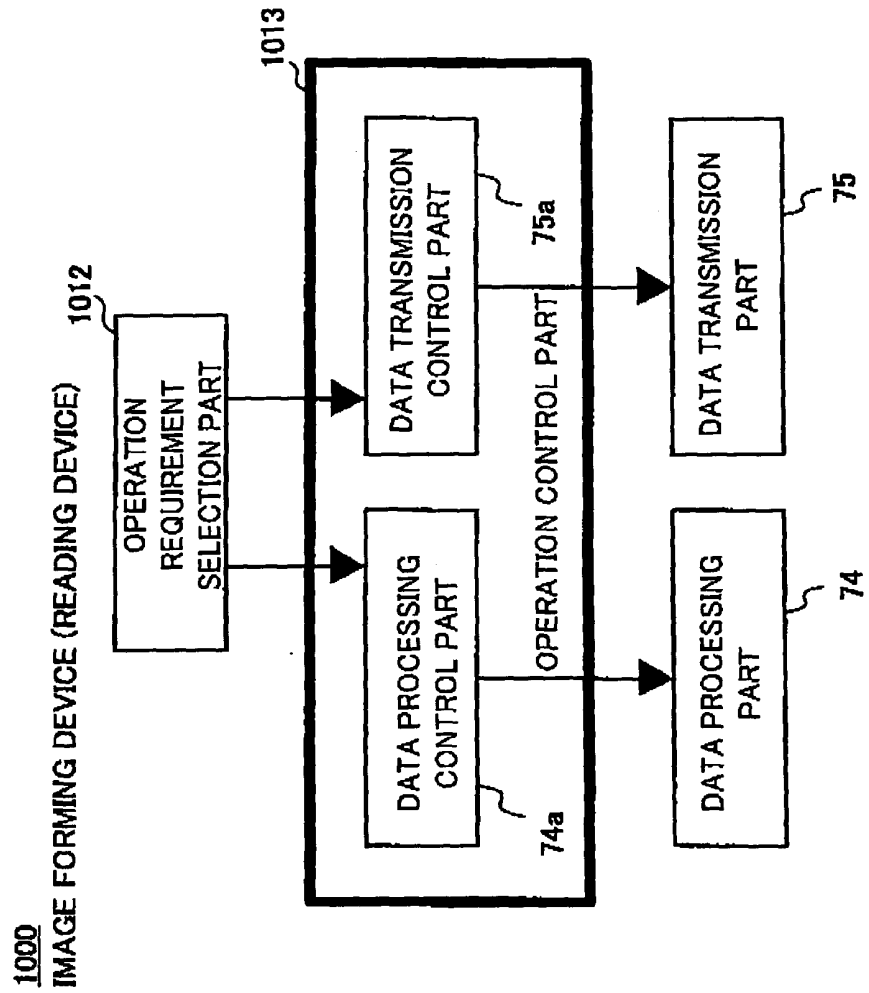


FIG. 76

